



(43) 国際公開日
2001 年 8 月 9 日 (09.08.2001)

PCT

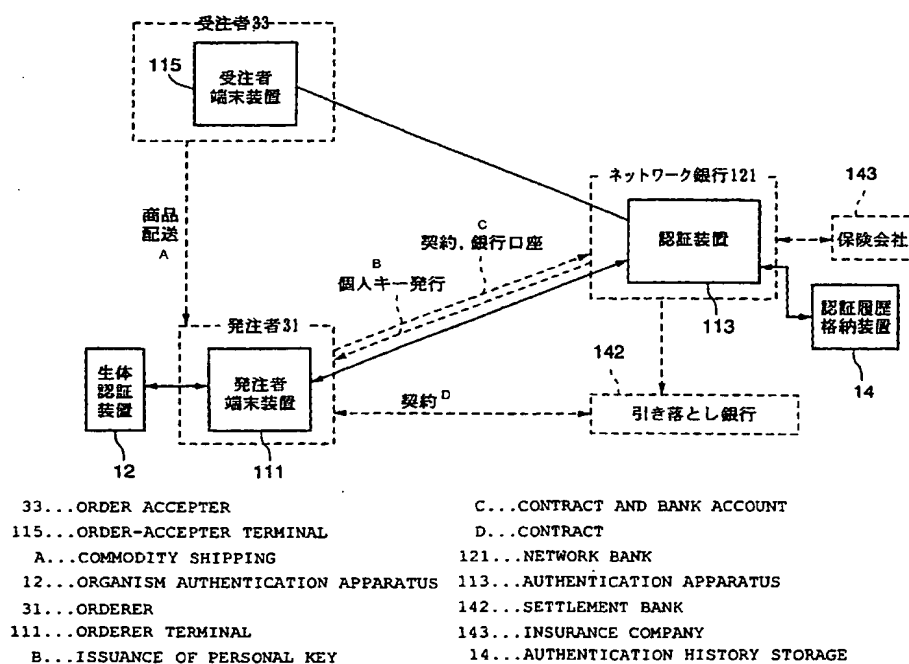
(10) 国際公開番号
WO 01/57750 A1

- | | | |
|----------------|----------------------------------|--|
| (51) 国際特許分類: | G06F 17/60, G09C 1/00, H04L 9/00 | (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP). |
| (21) 国際出願番号: | PCT/JP01/00772 | |
| (22) 国際出願日: | 2001 年2 月2 日 (02.02.2001) | (72) 発明者; および |
| (25) 国際出願の言語: | 日本語 | (75) 発明者/出願人 (米国についてのみ): 金巻裕史 (KANEMAKI, Hirofumi) [JP/JP]. 中村嘉秀 (NAKA-MURA, Yoshihide) [JP/JP]. 佐竹 清 (SATAKE, Sei) [JP/JP]. 齋藤 真 (SAITO, Makoto) [JP/JP]. 橋本主税 (HASHIMOTO, Chikara) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). |
| (26) 国際公開の言語: | 日本語 | |
| (30) 優先権データ: | | (74) 代理人: 佐藤隆久 (SATO, Takahisa); 〒111-0052 東京都台東区柳橋2丁目4番2号 宮木ビル4階 創造国際特許事務所 Tokyo (JP). |
| 特願2000-24619 | 2000 年2 月2 日 (02.02.2000) | JP |
| 特願2000-209674 | 2000 年7 月11 日 (11.07.2000) | JP |
| 特願2000-209675 | 2000 年7 月11 日 (11.07.2000) | JP |
| 特願2000-234741 | 2000 年8 月2 日 (02.08.2000) | JP |
| 特願2000-234752 | 2000 年8 月2 日 (02.08.2000) | JP |
| 特願2000-238077 | 2000 年8 月7 日 (07.08.2000) | JP |
| 特願2000-370519 | 2000 年12 月5 日 (05.12.2000) | JP |
| 特願 2000-379361 | | |
| | 2000 年12 月13 日 (13.12.2000) | JP |
| 特願2001-22436 | 2001 年1 月30 日 (30.01.2001) | JP |
| | | (81) 指定国 (国内): CN, US. |
| | | (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR). |
| | | 添付公開書類: |
| | | — 国際願査報告書 |

〔続葉有〕

(54) Title: AUTHENTICATION SYSTEM

(54) 発明の名称: 認証システム



(57) Abstract: An authentication apparatus for preventing unauthorized authentication using personal ID information about a person that another person fraudulently obtains. The authentication apparatus (50), in response to an authentication request from an orderer terminal (11), receives personal ID information (ID1) about an orderer (31), personal ID information (ID2) about an order-accepter (33), and transaction information, communicates with an order-accepter terminal (15), and sends authentication information representing the legitimacy of the order-accepter (33) to the orderer terminal (11).

〔統葉有〕

WO 01/57750 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

不正に取得した他人の個人ID情報に基づいて不正な認証手続が行われることを回避する認証装置を提供する。認証装置50は、発注者端末装置11からの認証要求によって、発注者31の個人ID情報ID1と、受注者33の個人ID情報ID2と、取り引き情報とを受信し、受注者端末装置15との間の通信を行った後に、受注者33の正当性を示す認証情報を発注者端末装置11に送信する。

明 細 書

認証装置、認証システムおよびその方法、処理装置、通信装置、
通信制御装置、通信システムおよびその方法、情報記録方法およびその装置、
情報復元方法およびその装置、その記録媒体

技術分野

本発明は、他人の個人ID情報を不正に用いた手続を防止できる認証装置、認証システムおよびその方法、処理装置、通信装置、通信制御装置、通信システムおよびその方法、記録媒体に保持される情報の秘匿性を高めることができる情報記録方法およびその装置、情報復元方法およびその装置並びに記録媒体に関する。

背景技術

インターネットなどのネットワークを介した電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行う受注者サーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ID情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

また、近年、電子商取引の発達に伴い、ユーザの個人ID情報や暗証番号、取引の履歴情報、ユーザの名前、住所、経歴および職業などの個人情報な

どの秘匿性のある情報を、サーバ装置や端末装置などが管理する場合が多くなっている。

サーバ装置や端末装置では、例えば、特開平 1 1 - 2 7 2 6 8 1 号公報に示されるように、上述したような秘匿性のある情報を、所定の暗号鍵で暗号化して、コンピュータに内蔵された HDD (Hard Disk Drive) や、携帯性のある CD-R OM、フロッピーディスク、PC カードなどの記録媒体に記録している。

しかしながら、上述したネットワークを介した従来の電子商取引では、発注者および受注者の当事者間でのみ取り引きが行われることから、偽発注および商取引情報の改竄などの不正を取り締まりことが困難であるという問題がある。

また、このような電子商取引について第 3 者が認証を行う場合でも、他人の個人 ID 情報を用いてネットワークを介して行われる不正な手続（いわゆる、なりすまし）が行われる可能性があるという問題がある。

また、上述したような電子商取引が普及すると、複数の認証機関が、電子商取引の認証業務を行うことになる。この場合に、同じ電子商取引に参加した利用者が、それぞれ異なる認証機関と契約をしている場合に、どのようにして当該電子商取引の正当性を認証するかが課題となる。

この場合に、同じ電子商取引に参加した利用者が契約した複数の認証機関で、利用者の情報を共有することで、上述した課題に対処できるが、利用者の個人情報、他の機関に漏れてしまうという問題がある。

また、家庭内に複数の端末装置を設けた場合に、外部のネットワークを介して行われる電子商取引やセキュリティに関する機能を端末装置毎に持たせると、効率が悪いと共に、例えば家庭単位で通信履歴を管理するときに不便である。

また、上述した従来のサーバ装置や端末装置では、通常、秘匿性のある情報を単体の記録媒体に記録しており、その記録媒体が盗まれたり、不正にコピーされると、当該情報の秘匿性が失われてしまうという問題がある。

このような秘匿性のある情報は、通常、暗号化されて記録媒体に記録されるが

、暗号化は復号（解読）される可能性があり、秘匿性を保持する上で十分ではない。

また、近年、公開鍵暗号方式を用いて生成した個人認証情報（PKI 情報）を小型のスマートカード（スマートメディア）に記憶し、当該スマートカードを用いて個人認証を行う場合があるが、このような個人認証情報は、印鑑証明と同等の効力を有していることから、スマートカードが盗難あるいは紛失された場合の被害が大きいという問題がある。

このような問題を回避するために、スマートカードの使用に際して、パスワードの照合を行うことが考えられるが、使い勝手が悪いという問題がある。

また、認証装置は、ネットワークを介した取引を認証する際に、個々の商取引を識別するトランザクション ID を生成して使用するが、商店などが故意または過失で、当該トランザクション ID を複数回用いて、同じ取引について、請求を行い、顧客の口座から重複した引き落としが行われることがあるという問題がある。

発明の開示

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人 ID 情報に基づいて不正な手続が行われることを回避する認証装置、認証システムおよびその方法を提供することを目的とする。

また、本発明は、異なる認証機関と契約した利用者相互間の取引の認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供することを目的とする。

また、本発明は、複数の端末装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提

供することを目的とする。

また、本発明は、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法、情報復元方法およびそれらの装置と記録媒体を提供することを目的とする。

また、本発明は、個人認証機能を持つ携帯型メモリ装置を用いて認証を行う場合に、煩雑な手続きを行うことなく、その安全性を高めることができる認証方法およびその装置を提供することを目的とする。

また、本発明は、商店などによって、トランザクションIDを用いて、同じ取り引きについて顧客の口座から複数回の引き落としが行われることを回避できる認証装置、認証システムおよびその方法を提供することを目的とする。

上述した従来技術の問題点を解決し、上述した目的を達成するために、

第1の発明の認証装置は、ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証装置であって、第1の取り引き者の個人キー情報および取り引き内容を示す情報を含む第1の要求を、前記第1の取り引き者から受信する第1の受信手段と、前記第1の要求に含まれる前記個人キー情報に基づいて前記第1の取り引き者の正当性を認証して第1の認証情報を生成する第1の認証手段と、前記第1の要求から前記第1の取り引き者の個人キー情報を除去した情報と、前記第1の認証情報とを含む第2の要求を前記第2の取り引き者に送信する第1の送信手段と、前記第2の要求に対しての応答を前記第2の取り引き者から受信する第2の受信手段と、前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、前記第2の認証情報を前記第1の取り引き者に送信する第2の送信手段とを有する。

第1の発明の認証装置の作用は以下になる。

第1の受信手段によって、第1の取り引き者の個人キー情報および取り引き内容を示す情報を含む第1の要求が、前記第1の取り引き者から受信される。

次に、第1の認証装置によって、前記第1の要求に応じて、前記第1の取り引

き者の正当性が認証され、第 1 の認証情報が生成される。

次に、第 1 の送信手段によって、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求が前記第 2 の取り引き者に送信される。

そして、第 2 の受信手段によって、前記第 2 の要求に対しての応答が前記第 2 の取り引き者から受信される。

次に、第 2 の認証手段によって、前記応答に応じて、前記第 2 の取り引き者の正当性が認証され、第 2 の認証情報が生成される。

次に、第 2 の送信手段によって、前記第 2 の認証情報が前記第 1 の取り引き者に送信される。

第 1 の発明の認証装置によれば、第 1 の送信手段から第 2 の取り引き者に送信される第 2 の要求には、前記第 1 の取り引き者の個人キー情報が含まれていないため、第 2 の取り引き者に、第 1 の取り引き者の課金に係わる情報が漏れることを回避できる。

第 2 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムであって、第 1 の取り引き者が使用する第 1 の通信装置と、第 2 の取り引き者が使用する第 2 の通信装置と、前記取り引きを認証する認証装置とを有し、前記認証装置は、第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記取り引き

の正当性を示す第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段とを有する。

第 2 の発明の認証システムの前記認証装置の作用は前述した第 4 の発明の認証装置の作用と同じである。

第 3 の発明の認証方法は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証方法であって、第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信し、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成し、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信し、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信し、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成し、前記第 2 の認証情報を前記第 1 の取り引き者に送信する。

第 4 の発明の認証装置は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証装置であって、第 1 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求を第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段とを有する。

第 4 の発明の認証装置の作用は以下ようになる。

第 1 の受信手段によって、第 1 の取り引き者の個人識別情報および取り引き内

容を示す情報を含む第 1 の要求が、前記第 1 の取り引き者から受信される。

次に、第 1 の認証装置によって、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性が認証され、第 1 の認証情報が生成される。

次に、第 1 の送信手段によって、前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求が前記第 2 の取り引き者に送信される。

そして、第 2 の受信手段によって、前記第 2 の要求に対しての応答が前記第 2 の取り引き者から受信される。

次に、第 2 の認証手段によって、前記応答に応じて、前記第 2 の取り引き者の正当性が認証され、第 2 の認証情報が生成される。

次に、第 2 の送信手段によって、前記第 2 の認証情報が前記第 1 の取り引き者に送信される。

上述したように、第 4 の発明によれば、第 1 の取り引き者と第 2 の取り引き者とが通信を行って取り引きを行う場合に、第 1 の取り引き者および第 2 の取り引き者以外の第 3 者が管理する当該認証装置を用いることで、第 1 の取り引き者の正当性を客観的に認証した結果である第 1 の認証情報を第 2 の取り引き者に送信し、第 2 の取り引き者の正当性を客観的に認証した結果である第 2 の認証情報を第 1 の取り引き者に送信することができ、取り引きの信頼性を高めることが可能になる。

第 4 の発明は、好ましくは、前記第 1 の受信手段は、前記第 1 の取り引き者の個人キー情報をさらに含む前記第 1 の要求を受信し、前記第 1 の認証手段は、前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証する。

ここで、前記第 1 の取り引き者の前記個人キー情報は、前記第 1 の取り引き者の課金に係わる情報である。

第 4 の発明の認証装置は、好ましくは、前記第 1 の送信手段は、前記第 1 の取り引き者の前記個人キー情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する。

第4の発明の認証装置は、好ましくは、前記取り引きの履歴を示す履歴情報を記憶する記憶手段をさらに有する。

第5の発明の認証システムは、ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証システムであって、第1の取り引き者が使用する第1の通信装置と、第2の取り引き者が使用する第2の通信装置と、前記取り引きを認証する認証装置とを有し、前記第1の通信装置は、第1の取り引き者の個人識別情報および取り引き内容を示す情報を含む第1の要求を前記認証装置に送信し、前記認証装置は、前記第1の取り引き者から前記第1の要求を受信する第1の受信手段と、前記第1の要求に応じて、前記第1の取り引き者の正当性を認証して第1の認証情報を生成する第1の認証手段と、前記第1の認証情報および前記取り引きの内容を示す情報を含む第2の要求を前記第2の取り引き者に送信する第1の送信手段と、前記第2の要求に対しての応答を前記第2の取り引き者から受信する第2の受信手段と、前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、前記第2の認証情報を前記第1の取り引き者に送信する第2の送信手段とを有する。

ここで、第5の発明の認証システムの前記認証装置の作用は前述した第1の発明の認証装置の作用と同じである。

第6の発明の認証方法は、ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証方法であって、第1の取り引き者の個人識別情報および取り引き内容を示す情報を含む第1の要求を、前記第1の取り引き者から受信し、前記第1の要求に応じて、前記第1の取り引き者の正当性を認証して第1の認証情報を生成し、前記第1の認証情報および前記取り引きの内容を示す情報を含む第2の要求を第2の取り引き者に送信し、前記第2の要求に対しての応答を前記第2の取り引き者から受信し、前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成し、前記第2の認証情報を前記第1の取り引き者に送信する。

第 7 の発明の認証装置は、第 1 の取り引き者に関する情報を保持し、第 2 の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証装置であって、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果を示す第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける送受信手段と、前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、前記所定の応答を受けた場合に、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される第 2 の署名情報であって、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成する署名作成手段とを有する。

第 7 の発明の認証装置の作用は以下ようになる。

送受信手段、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求を受ける。

そして、当該第 2 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求が、前記送受信手段から前記第 2 の認証装置に送信される。

次に、送受信手段は、前記第 2 の要求に応じた第 1 の署名情報を前記第 2 の認証装置から受信する。

次に、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を、前記送受信手段から前記第 2 の取り引き者が使用する装置に送信する。

次に、送受信手段は、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する

る装置から所定の応答を受ける。

前記送受信手段が前記所定の応答を受けると、記憶手段に、前記取り引きの履歴が記憶される。

また、前記送受信手段が前記所定の応答を受けると、署名作成手段によって、前記取り引きの正当性を認証する第2の署名情報が作成され、当該第2の署名情報が、前記送受信手段を介して前記第1の取り引き者が使用する装置に送信される。

第7の発明の認証装置は、好ましくは、暗号化手段をさらに有し、前記送受信手段は、前記第2の取り引き者との間の通信に用いる暗号鍵を前記第2の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第1の署名情報とを、前記第2の取り引き者が使用する装置に送信する。

第7の発明の認証装置は、好ましくは、前記送受信手段は、前記他の認証装置が前記第2の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第2の取り引き者が使用する装置から受け、前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する。

第7の発明の認証装置は、好ましくは、前記送受信手段は、前記第1の要求に含まれる前記取り引き内容に関する情報のうち、前記第1の取り引き者の課金に係わる情報以外の情報と、前記第1の署名情報とを含む第3の要求を前記第2の取り引き者が使用する装置に送信する。

第7の発明の認証装置は、好ましくは、前記送受信手段は、前記第1の要求に含まれる前記取り引き内容に関する情報と、前記第1の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第3の要求を前記第2の取り引き者が使用する装置に送信する。

第7の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

第7の発明の認証装置は、好ましくは、前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

第7の発明の認証装置は、好ましくは、前記送受信手段は、前記第2の取り引き者が前記第1の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第2の取り引き者が使用する装置から、前記記所定の応答を受ける。

第8の発明の認証システムは、ネットワークを介して少なくとも2者間で行われた取り引きを認証する認証システムであって、第1の取り引き者に関する取り引きを認証する第1の認証装置と、第2の取り引き者に関する取り引きを認証する第2の認証装置とを有し、前記第1の認証装置は、前記取り引き内容を示す情報と前記第2の取り引き者を特定する情報とを含む前記第1の取り引き者による第1の要求に応じて、前記第2の取り引き者を特定する情報を含む第2の要求を前記第2の認証装置に送信し、前記第2の要求に応じた前記第2の認証装置からの第1の署名情報を受信し、前記第1の要求に含まれる前記取り引き内容に関する情報と前記第1の署名情報とを含む第3の要求を前記第2の取り引き者が使用する装置に送信し、当該第3の要求に応じて前記第2の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性を認証する第2の署名情報を前記第1の取り引き者に提供する。

第8の発明の認証システムは、前記第1の認証装置は、暗号化手段をさらに有し、前記送受信手段は、前記第2の取り引き者との間の通信に用いる暗号鍵を前記第2の要求に応じて前記第2の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第1の署名情報とを、前記第2の取り引き者が使用する装置に送信する。

第9の発明の認証方法は、第1の取り引き者に関する取り引きを認証する第1の認証装置と、第2の取り引き者に関する取り引きを認証する第2の認証装置とを用いて、ネットワークを介して行われる前記第1の取り引き者と前記第2の取

り引き者との間の取り引きに関する認証を行う認証方法であって、前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を送信し、前記第 2 の要求に応じて、前記第 2 の認証装置からの前記第 1 の認証装置に、当該第 2 の認証装置による認証結果を示す第 1 の署名情報を送信し、前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を送信し、当該第 3 の要求に応じて、前記第 2 の取り引き者が使用する装置から前記第 1 の認証装置に所定の応答を出し、前記所定の応答に応じて、前記第 1 の認証装置は、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成し、当該第 2 の署名情報を、前記第 1 の取り引き者が使用する装置に送信する。

第 10 の発明の認証方法は、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証方法であって、前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 1 の取り引き者の個人キー情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 1 の要求から前記個人キーを除去した第 2 の要求を送信し、前記第 2 の要求に応じて、前記取り引きの内容を示す情報を含む第 3 の要求を、前記第 2 の認証装置から前記第 2 の取り引き者が使用する装置に送信し、前記第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から前記第 2 の認証装置に第 1 の応答を送信し、前記第 1 の応答に応じて、前記第 2 の認証装置から前記第 1 の認証装置に、前記第 2 の取り引き者への支払い方法を示す支払い方法情報

を含む第 2 の応答を送信し、前記第 1 の認証装置は、前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取り引き者との間の前記取り引き者に関する支払いを管理する。

また、第 10 の発明の認証方法は、好ましくは、前記第 1 の認証装置は、前記取り引きに関して、前記第 1 の取り引き者から支払い金を受けるための処理と、前記支払い金の一部を前記取り引きに応じて前記第 2 の取り引き者に支払う処理と、前記支払い金の残りを手数料として受け取る処理と行う。

また、第 10 の認証方法は、好ましくは、前記第 1 の認証装置は、前記第 1 の要求に応じて、前記第 2 の取り引き者が前記第 2 の認証装置と契約しているか否かを前記第 2 の認証装置に問い合わせ、契約している旨の回答を前記第 2 の認証装置から受信した場合に、前記第 2 の要求を前記第 2 の認証装置に送信する。

また、第 10 の発明の認証方法は、好ましくは、前記第 1 の認証装置は、前記第 2 の応答を受信すると、前記取り引き者について当該第 1 の認証装置が行った認証結果を含む署名情報を含む第 3 の応答を、前記第 1 の取り引き者が使用する装置に送信する。

また、第 10 の発明の認証方法は、好ましくは、前記第 1 の認証装置は、当該第 1 の認証装置に対応する秘密鍵を用いて、前記第 3 の応答を暗号化して前記第 1 の取り引き者が使用する装置に送信する。

また、第 10 の発明の認証方法は、好ましくは、前記第 1 の認証装置は、前記取り引きについて当該第 1 の認証装置が行った認証結果を示す署名情報をさらに含む前記第 2 の要求を前記第 2 の認証装置に送信する。

また、第 10 の発明の認証方法は、好ましくは、前記第 2 の認証装置は、前記取り引きについて当該第 2 の認証装置が行った認証結果を示す署名情報をさらに含む前記第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する。

また、第 10 の発明の認証方法は、好ましくは、前記第 1 の認証装置は、当該第 1 に認証装置に対応する秘密鍵を用いて、前記第 2 の要求を暗号化して前記第

2の認証装置に送信する。

また、第10の発明の認証方法は、好ましくは、前記第2の認証装置は、当該第2の認証装置に対応する秘密鍵を用いて、前記第3の要求を暗号化して前記第2の取り引き者が使用する装置に送信する。

また、第10の発明の認証方法は、好ましくは、前記第2の取り引き者の装置は、当該第2の取り引き者の秘密鍵を用いて、前記第1の応答を暗号化して前記第2の認証装置に送信する。

また、第10の発明の認証方法は、好ましくは、前記第2の認証装置は、当該第2に認証装置に対応する秘密鍵を用いて、前記第2の応答を暗号化して前記第1の認証装置に送信する。

また、第11の発明の認証装置は、第1の取り引き者に関する情報を保持し、第2の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第1の取り引き者と前記第2の取り引き者との間の取り引きに関する認証を行う認証装置であって、前記取り引き内容を示す情報と前記第1の取り引き者の個人キー情報と前記第2の取り引き者を特定する情報とを含む第1の要求を前記第1の取り引き者から受信し、前記第2の取り引き者への支払い方法を示す支払い方法情報を含む応答を前記他の認証装置から受信する受信手段と、前記第1の要求に応じて、前記第1の要求から前記個人キーを除去した第2の要求を前記他の通信装置に送信する送信手段と、前記支払い方法情報に基づいて、前記第1の取り引き者と前記第2の取り引き者との間の前記取り引き者に関する支払いを管理する課金手段とを有する。

第11の発明の認証装置の作用は以下になる。

まず、受信手段によって、前記取り引き内容を示す情報と前記第1の取り引き者の個人キー情報と前記第2の取り引き者を特定する情報とを含む第1の要求が受信される。

次に、送信手段によって、前記第1の要求に応じて、前記第1の要求から前記

個人キーを除去した第 2 の要求が前記他の通信装置に送信される。

次に、受信手段によって、前記第 2 の取り引き者への支払い方法を示す支払い方法情報を含む応答が前記他の認証装置から受信される。

次に、課金手段によって、前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取り引き者との間の前記取り引き者に関する支払いが管理される。

第 1 2 の発明の認証システムは、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを有し、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証システム方法であって、前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 1 の取り引き者の個人キー情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 1 の要求から前記個人キーを除去した第 2 の要求を送信し、前記第 2 の要求に応じて、前記取り引きの内容を示す情報を含む第 3 の要求を、前記第 2 の認証装置から前記第 2 の取り引き者が使用する装置に送信し、前記第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から前記第 2 の認証装置に第 1 の応答を送信し、前記第 1 の応答に応じて、前記第 2 の認証装置から前記第 1 の認証装置に、前記第 2 の取り引き者への支払い方法を示す支払い方法情報を含む第 2 の応答を送信し、前記第 1 の認証装置は、前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取り引き者との間の前記取り引き者に関する支払いを管理する。

第 1 3 の発明の認証方法は、認証装置において、ユーザの認証情報を第 1 の認証情報および第 2 の認証情報に分割し、前記第 2 の認証情報を記憶した携帯型メモリ装置を前記ユーザに提供し、前記携帯型メモリ装置にアクセス可能な端末装置から前記認証装置に認証情報要求を送信し、前記認証装置において、前記認証

情報要求が正当なユーザによるものであると判断した場合に、前記認証装置から前記端末装置に前記第 1 の認証情報を送信し、前記端末装置において、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とを用いて前記認証情報を復元する。

第 13 の発明の認証方法によれば、ユーザの個人を認証する認証情報のうち一部の第 2 の認証情報のみを携帯型メモリ装置に記憶することから、ユーザが携帯型メモリ装置を盗まれたり、落としたりした場合に、他人は、携帯型メモリ装置のみでは、不正な認証処理を行うことができない。このとき、認証情報の全体を得るには、認証装置において正当なユーザであるかの確認を行う必要がある。

第 13 の発明の認証方法は、好ましくは、前記認証情報要求は、前記第 1 の認証情報の送信先を指定した送信先情報を含み、前記認証装置は、前記送信先情報で指定された前記端末装置に、前記第 1 の認証情報を送信する。

第 13 の発明の認証方法は、好ましくは、前記認証装置は、前記ユーザに対応する送信先情報を予め記憶し、当該記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する。

第 13 の発明の認証方法は、好ましくは、前記端末装置は、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とが対応していると判断した場合に、前記受信した第 1 の認証情報を記憶して前記認証情報を復元する。

第 13 の発明の認証方法は、好ましくは、前記端末装置は、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とが対応していない場合に、その旨を示す通知を前記認証装置に送信する。

第 13 の発明の認証方法は、好ましくは、前記認証装置は、前記ユーザからの要求に応じて、前記認証情報を生成する。

第 1 3 の発明の認証方法は、好ましくは、前記認証情報は、公開鍵暗号を用いて作成された情報である。

第 1 3 の発明の認証方法は、好ましくは、前記携帯型メモリ装置は、スマートカードである。

第 1 4 の発明の認証方法は、認証情報を生成し、前記認証情報を第 1 の認証情報および第 2 に認証情報に分割し、前記第 2 の認証情報を記憶した携帯型メモリ装置をユーザに提供し、受信した認証情報要求が正当なユーザによるものであると判断した場合に、前記認証情報要求が指定する送信先に、前記第 1 の認証情報を送信する。

第 1 5 の発明の認証装置は、認証情報を生成し、前記認証情報を第 1 の認証情報および第 2 に認証情報に分割し、受信した認証情報要求が正当なユーザによるものであるか否かを判断する制御手段と、携帯型メモリ装置に前記第 2 の認証情報を書き込む書込手段と、前記携帯型メモリ装置のユーザから前記認証情報要求を受信する受信手段と、前記認証情報要求が正当なユーザによるものであると判断された場合に、前記第 1 の認証情報を前記認証情報要求によって指定された送信先に送信する送信手段とを有する。

第 1 5 の認証装置の作用は以下になる。

制御手段によって、ユーザの個人を認証するための認証情報が生成され、当該認証情報が第 1 の認証情報および第 2 に認証情報に分割される。

書込手段によって、携帯型メモリ装置に前記第 2 の認証情報が書き込まれる。

そして、受信手段が前記携帯型メモリ装置のユーザから認証情報要求を受信すると、制御手段によって、前記受信した認証情報要求が正当なユーザによるものであるか否かが判断される。

そして、前記認証情報要求が正当なユーザによるものであると判断された場合に、送信手段によって、前記第 1 の認証情報が前記認証情報要求によって指定さ

れた送信先に送信される。

第 16 の発明の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段とを有する。

第 16 の発明の通信装置の作用は以下になる。

例えば、利用者が他の通信装置を操作して、利用者を識別するための個人識別情報を含む要求を送信する。

当該要求は、受信手段で受信される。

次に、処理手段において、当該受信した要求に応じた所定の処理が行われる。

次に、送信手段によって、前記受信した要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記処理の結果が送信される。

第 16 の発明の通信装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、前記通信装置は、前記受信した要求に含まれる前記個人識別情報を復号する復号手段をさらに有する。

また、第 16 の発明の通信装置は、好ましくは、前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である。

また、第 16 の発明の通信装置は、好ましくは、前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である。

また、第 16 の発明の通信装置は、好ましくは、前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を

一意に識別するための個人識別情報である。

また、第 16 の発明の通信装置は、好ましくは、前記処理は、認証処理である。

第 17 の発明の通信システムは、ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を有する通信システムであって、前記第 1 の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する第 1 の受信手段と、前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第 1 の送信手段とを有し、前記第 2 の通信装置は、前記要求を前記第 1 の通信装置に送信する第 2 の送信手段と、前記処理の結果を前記第 1 の通信装置から受信する第 2 の受信手段と、当該受信した認証処理の結果を出力する出力手段とを有する。

第 18 の発明の通信方法は、ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を用いた通信方法であって、利用者を識別するための個人識別情報を含む要求を、前記第 2 の通信装置から前記第 1 の通信装置に送信し、前記第 1 の通信装置において、前記要求に応じて所定の処理を行い、前記第 1 の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する。

第 19 の発明の認証装置は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証装置であって、第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証

手段と、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段と、前記第 1 の要求を受信したときに、取り引き識別情報を発行する取り引き識別情報発行手段と、前記取り引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴を管理する取り引き履歴管理手段とを有する。

第 19 の発明の認証装置の作用は以下になる。

第 1 の受信手段によって、第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求が、前記第 1 の取り引き者から受信される。

これにより、取り引き識別情報発行手段によって、取り引き識別情報が発行される。

次に、第 1 の認証手段によって、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性が認証され、第 1 の認証情報が生成される。

次に、第 1 の送信手段によって、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と前記第 1 の認証情報とを含む第 2 の要求が、第 2 の取り引き者に送信される。

次に、第 2 の受信手段によって、前記第 2 の要求に対しての応答が前記第 2 の取り引き者から受信される。

次に、第 2 の認証手段によって、前記応答に応じて、前記第 2 の取り引き者の正当性が認証され、第 2 の認証情報が生成される。

次に、第 2 の送信手段によって、前記第 2 の認証情報が前記第 1 の取り引き者に送信される。

本発明の認証装置では、取り引き履歴管理手段によって、前記取り引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴が管理される。

そのため、取り引き識別管理手段によって管理された履歴に基づいて、取り引き識別情報を不正に用いた第 2 の取り引き者の第 2 の要求を検出できる。

また、第 19 の発明の認証装置は、好ましくは、前記取り引き履歴管理手段は、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信のそれぞれについて履歴情報を生成し、当該履歴情報を前記取り引き識別情報に関連付けて記憶する。

また、第 19 の発明の認証装置は、好ましくは、前記送信手段は、前記取り引き識別情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する。

また、第 19 の発明の認証装置は、好ましくは、前記第 2 の認証手段は、前記応答に含まれる前記取り引き識別情報と、前記取り引き履歴管理手段が管理する前記履歴とに基づいて、前記応答の正当性を認証する。

また、第 19 の発明の認証装置は、好ましくは、前記取り引きに係わる決済処理を行う決済処理手段をさらに有し、前記取り引き履歴管理手段は、前記決済処理の終了後に、決済処理が終了したことを示す履歴情報を前記取り引き識別情報に関連付けて記憶する。

また、第 19 の発明の認証装置は、好ましくは、前記第 1 の取り引き者の個人キー情報は前記第 1 の取り引き者の課金に係わる情報である。

第 20 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムであって、第 1 の取り引き者が使用する第 1 の通信装置と、第 2 の取り引き者が使用する第 2 の通信装置と、前記取り引きを認証する認証装置とを有し、前記認証装置は、前記第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に含まれる前記個人キー情

報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む前記第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段と、前記第 1 の要求を受信したときに、取り引き識別情報を発行する取り引き識別情報発行手段と、前記取り引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴を管理する取り引き履歴管理手段とを有する。

第 2 1 の発明の認証方法は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証方法であって、第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信し、当該受信に応じて取り引き識別情報を発行し、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成し、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信し、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信し、

前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成し、前記第 2 の認証情報を前記第 1 の取り引き者に送信し、前記取り引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴を管理する。

また、第 2 1 の発明の認証方法は、好ましくは、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信のそれぞれについて履歴情報を生成し、当該履歴情報を前記取り引き識別情報に関連付けて記憶する。

また、第 2 1 の発明の認証方法は、好ましくは、前記取り引き識別情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する。

第 2 2 の発明の通信制御装置は、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、前記第 1 の通信装置を識別するための装置識別情報を記憶する記憶手段と、前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を前記第 2 の通信装置に送信する送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する受信手段と、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段とを有する。

第 2 2 の発明の通信制御装置の作用は以下のようになる。

送信手段、第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を第 2 の通信装置に送信する。

そして、受信手段が、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する。

次に、制御手段によって、前記受信した応答に含まれる前記装置識別情報と記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する。

第 2 2 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う。

第 2 2 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含

まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う。

また、第２２の発明の通信制御装置は、好ましくは、前記送信手段は、前記第１の通信装置から受信した個人識別情報と、当該第１の通信装置に対応する前記装置識別情報とを含む前記要求を前記第２の通信装置に送信する。

また、第２２の発明の通信制御装置は、好ましくは、前記記憶手段は、前記第１の通信装置から受信した前記装置識別情報を記憶する。

また、第２２の発明の通信制御装置は、好ましくは、前記記憶手段は、当該通信制御装置の電源が投入されたときに前記第１の通信装置から受信した前記装置識別情報を記憶する。

また、第２２の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置と前記第２の通信装置との間の通信履歴を前記記憶手段に書き込む。

また、第２２の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記第２の通信装置の処理結果を、前記要求の送信元の前記第１の通信装置に送信する。

また、第２２の発明の通信制御装置は、好ましくは、前記制御手段は、前記受信手段から受信した情報に応じて、待機状態にある前記第１の通信装置が動作状態になるように制御する。

また、第２２の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置が接続されたネットワークと、前記第２の通信装置が接続されたネットワークとの間の通信を制御する。

また、第２２の発明の通信制御装置は、好ましくは、前記装置識別情報は、前記第１の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である。

また、第 2 2 の発明の通信制御装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

第 2 3 の発明の通信システムは、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、前記通信制御装置は、前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記憶手段と、前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段とを有し、前記第 2 の通信装置は、前記要求を受信する第 2 の受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段とを有する。

第 2 4 の発明の通信方法は、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当該第 1 の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、前記第 2

の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する。

第 25 の発明の認証装置は、認証要求に応じて認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

第 25 の発明の認証装置の作用は以下のようになる。

例えば、利用者が端末装置などを操作して当該端末装置から送信された、利用者を識別するための個人識別情報と、認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求が受信手段で受信される。

次に、当該受信された前記認証要求に応じた認証処理が認証処理手段で行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とが対応付けて送信手段から送信される。

第 25 の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記

個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

また、第 25 の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する。

また、第 25 の発明の認証装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

また、第 25 の発明の認証装置は、好ましくは、前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である。

第 26 の発明の認証装置は、ネットワークを介して行われる取引に関する認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、取引の内容を示す取引情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取引を行う利用者による前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記受信した認証要求に含まれる前記取引情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

第 26 の発明の認証装置の作用は以下のようなになる。

利用者を識別するための個人識別情報と、取引の内容を示す取引情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取引を行う利用者による前記認証要求が受信手段で受信される。

次に、認証処理手段によって、前記受信した認証要求に含まれる前記取り引き情報が前記認証要求によって指定された利用者の装置に送信され、当該指定された利用者の装置からの応答に応じて、所定の認証処理が行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信手段から送信される。

第26の発明の認証装置は、好ましくは、前記認証処理手段は、前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する。

第26の発明の認証装置は、好ましくは、前記記憶手段は、前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する。

第26の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

また、第26の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第3の識別情報をさらに含む前記認証要求を受信する。

また、第26の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

第27の発明の処理装置は、ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、認証要求の送信元の装置を識別するための識別情報を含む認証応答を受

信する受信手段と、前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段とを有する。

第 27 の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する。

また、第 27 の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引きの取り引き先の装置に所定の通知を行う。

第 28 の発明の認証システムは、ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、前記認証装置は、利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段とを有し、前記処理装置は、前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、前記認証応答を受信する受信手段と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段とを有する。

第 29 の発明の認証方法は、ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、前記認証装置において前記認証要求に応じて認証処理

を行い、前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する。

第30の発明の情報記録方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

第30の発明の情報記録方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第30の発明の情報記録方法は、好ましくは、前記所定の情報を暗号化し、当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する。

また、第30の発明の情報記録方法は、好ましくは、前記複数のモジュールをそれぞれ暗号化し、当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

第31の発明の情報復元方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、当該読み出したモジュールを合成して前記所定の情報を復元する。

第31の発明の情報復元方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第 3 1 の発明の情報復元方法は、好ましくは、前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する。

また、第 3 1 の発明の情報復元方法は、好ましくは、前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する。

第 3 2 の発明の情報記録装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段とを有する。

第 3 3 の発明の情報復元装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段とを有する。

第 3 4 の発明の記録媒体は、コンピュータによって読み取り可能であり、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録されている。

図面の簡単な説明

図 1 は、本発明の第 1 実施形態に係わるトランザクション認証システムの全体構成図である。

図 2 は、図 1 に示す発注者端末装置の機能ブロック図である。

図 3 は、図 1 に示す認証装置の機能ブロック図である。

図 4 は、図 1 に示す受注者端末装置の機能ブロック図である。

図 5 A ～ 5 D は、図 1 に示すトランザクション認証システムの動作を説明するための図である。

図6は、本発明の第2実施形態に係わるトランザクション認証システムの全体構成図である。

図7は、図6に示す発注者端末装置の機能ブロック図である。

図8は、図6に示す認証装置の機能ブロック図である。

図9は、図6に示す受注者端末装置の機能ブロック図である。

図10A～10Dは、図6に示すトランザクション認証システムの動作を説明するための図である。

図11は、本発明の第3実施形態のトランザクション認証システムの全体構成図である。

図12は、図11に示す発注者端末装置の構成図である。

図13は、図11に示す受注者端末装置の構成図である。

図14は、図11に示す認証装置(A)の構成図である。

図15は、図11に示す認証装置(B)の構成図である。

図16A～16Fは、図11に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図17は、本発明の第4実施形態のトランザクション認証システムの全体構成図である。

図18は、図17に示す発注者端末装置の構成図である。

図19は、図17に示す受注者端末装置の構成図である。

図20は、図17に示す認証装置(A)の構成図である。

図21は、図17に示す認証装置(B)の構成図である。

図22A～22Fは、図17に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図23A～23Fは、図17に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図24は、本発明の第5実施形態の認証システムの全体構成図である。

図 2 5 は、図 2 4 に示す端末装置の機能ブロック図である。

図 2 6 は、図 2 4 に示す認証装置の機能ブロック図である。

図 2 7 は、図 2 4 に示す認証システムにおいて、ネットワーク銀行が認証情報の一部が記憶されたスマートカードを作成し、これをユーザに送付するまでの動作例を説明するためのフローチャートである。

図 2 8 は、図 2 4 に示す認証システムにおいて、ユーザがスマートカードを用いて、端末装置で認証情報を得るときの動作例を説明するためのフローチャートである。

図 2 9 は、図 2 4 に示す認証システムにおいて、ユーザがスマートカードを用いて、端末装置で認証情報を得るときの動作例を説明するためのフローチャートである。

図 3 0 は、本発明の第 6 実施形態のトランザクション認証システムの全体構成図である。

図 3 1 は、図 3 0 に示す発注者端末装置の構成図である。

図 3 2 は、図 3 0 に示す受注者端末装置の構成図である。

図 3 3 は、図 3 0 に示す認証装置の構成図である。

図 3 4 A ～ 3 4 D は、発注者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

図 3 5 A ～ 3 5 D は、不正者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

図 3 6 は、本発明の第 7 実施形態におけるトランザクション認証システムの構成を示した構成図である。

図 3 7 は、図 3 6 に示す発注者端末装置の機能ブロック図である。

図 3 8 は、図 3 6 に示す認証装置の機能ブロック図である。

図 3 9 は、図 3 6 に示す受注者端末装置の機能ブロック図である。

図 4 0 は、図 3 6 に示すトランザクション認証システムの全体動作を説明する

ための図である。

図41は、図36に示すトランザクション認証システムの全体動作を説明するための図である。

図42は、本発明の第8実施形態のトランザクション認証システムの全体構成図である。

図43は、図42に示すホームネットワークシステムを説明するための図である。

図44は、図43に示すホームゲートウェイの構成図である。

図45は、図43に示す受注者端末装置の構成図である。

図46は、図42に示す認証装置の構成図である。

図47A～47Fは、正当者が認証要求を出した場合の図42に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図48A～48Eは、不正者が認証要求を出した場合の図35に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図49は、本発明の第9実施形態に係わるトランザクション認証システムの全体構成図である。

図50は、図49に示す発注者端末装置の構成図である。

図51は、図49に示す受注者端末装置の構成図である。

図52は、図49に示す認証装置の構成図である。

図53A～53Eは、図49に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

図54は、本発明の第10実施形態の情報記録装置の構成図である。

図55は、図54に示す情報記録装置における処理の情報の流れを説明するための図である。

図56は、図54に示す情報記録装置の処理のフローチャートである。

図57は、本発明の第11実施形態の情報復元装置の構成図である。

図 5 8 は、図 5 7 に示す情報復元装置における処理の情報の流れを説明するための図である。

図 5 9 は、図 5 7 に示す情報復元装置の処理のフローチャートである。

図 6 0 は、本発明の第 1 2 実施形態の情報記録装置の構成図である。

図 6 1 は、図 6 0 に示す情報記録装置における処理の情報の流れを説明するための図である。

図 6 2 は、図 6 0 に示す情報記録装置の処理のフローチャートである。

図 6 3 は、本発明の第 1 3 実施形態の情報復元装置の構成図である。

図 6 4 は、図 6 3 に示す情報復元装置における処理の情報の流れを説明するための図である。

図 6 5 は、図 6 4 に示す情報復元装置の処理のフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施形態に係わるトランザクション認証システムを図面を参照して説明する。

第 1 実施形態

図 1 は、本実施形態におけるトランザクション認証システム 1 0 1 の構成を示した構成図である。

トランザクション認証システム 1 0 1 は、発注者 3 1 が発注処理を行う発注者端末装置 1 1 1 と、発注者 3 1 の生体的特徴を利用して発注者 3 1 が本人であることを認証する生体認証装置 1 2 と、ネットワーク銀行（あるいはトランザクション認証局運営会社） 1 2 1 によって使用され、商取引情報の認証を行う認証装置 1 1 3 と、認証履歴を格納する認証履歴格納装置 1 4 と、受注者 3 3 が受注処理を行う受注者端末装置 1 1 5 とを有する。

本実施形態は、第 1 ～ 3 の発明に対応した実施形態であり、発注者端末装置 1 1 1 が本発明の第 1 の通信装置に対応し、認証装置 1 1 3 が本発明の認証装置に

対応し、受注者端末装置 1 1 5 が本発明の第 2 の通信装置に対応している。また、発注者 3 1 が本発明の第 1 の取り引き者に対応し、受注者 3 3 が本発明の第 2 の取り引き者に対応している。

〔発注者端末装置 1 1 1〕

図 2 は、発注者端末装置 1 1 1 の機能ブロック図である。

発注者端末装置 1 1 1 は、本システム利用の契約を行った一般利用者である発注者 3 1 が使用する端末装置である。

発注者端末装置 1 1 1 は、図 2 に示すように、認証要求入力部 1 1 1 a、認証要求送信部 1 1 1 b、認証応答受信部 1 1 1 c、認証要求暗号化部 1 1 1 d および認証応答復号部 1 1 1 e を有する。

認証要求入力部 1 1 1 a は、例えば、発注者 3 1 によるキーボードなどの操作に応じて、発注情報 a 1 および発注者個人キー情報 k 1（本発明の第 1 の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報 a 1 には、例えば、発注者 3 1 の名前、住所、連絡先、受注者 3 3 の個人 ID 情報 ID 2（本発明の第 2 の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部 1 1 1 b は、認証要求入力部 1 1 1 a に入力された発注情報 a 1 および発注者個人キー情報を含む認証要求 Inf 1（本発明の第 1 の要求）を認証装置 1 1 3 に送信する。

認証応答受信部 1 1 1 c は、認証装置 1 1 3 から認証応答 Inf 4 を受信する。

認証要求暗号化部 1 1 1 d は、認証要求 Inf 1 を暗号化する。

認証応答復号部 1 1 1 e は、認証応答 Inf 4 を復号する。

生体認証装置 1 2 は、いわゆるバイオメトリックス (biometrics) を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置 1

2に格納しておいた利用者（発注者31）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置12の記録装置は、外部から電氣的に切断されており、その情報が外部に流出しない構成となっている。

〔認証装置113〕

図3は、認証装置113の機能ブロック図である。

認証装置113は、本システムを運営するネットワーク銀行121が使用する装置である。

認証装置113は、図3に示すように、認証要求受信部113a、発注者認証部113b、要求生成部113c、要求送信部113d、応答受信部113e、受注者認証部113f、認証応答生成部113g、認証応答暗号化部113h、認証応答送信部113i、要求暗号化部113j、応答復号部113kおよび認証要求復号部113lを有する。

ここで、認証要求受信部113aが本発明の第1の受信手段に対応し、発注者認証部113bおよび要求生成部113cが本発明の第1の認証手段に対応し、要求送信部113dが本発明の第1の送信手段に対応し、応答受信部113eが本発明の第2の受信手段に対応し、受注者認証部113fおよび認証応答生成部113gが本発明の第2の認証手段に対応し、認証応答暗号化部113hが本発明の暗号化手段に対応し、認証応答送信部113iが本発明の第2の送信手段に対応し、要求暗号化部113jが本発明の暗号化手段に対応し、応答復号部113kが本発明の復号手段に対応し、認証要求復号部113lが本発明の復号手段に対応している。

認証要求受信部113aは、発注者端末装置111が送信した認証要求Inf1を受信する。

発注者認証部113bは、認証要求Inf1が含む発注者個人キー情報k1を

用いて発注者 3 1 の認証を行い、認証情報 A u 1 (本発明の第 1 の認証情報) を生成する。

要求生成部 1 1 3 c は、認証要求 I n f 1 から個人キー情報 k 1 を削除して情報 I n f 1 a を生成し、当該情報 I n f 1 a と認証情報 A u 1 とを含む要求 I n f 2 (本発明の第 2 の要求) を生成する。

要求送信部 1 1 3 d は、要求 I n f 2 を受注者端末装置 1 1 5 に送信する。

応答受信部 1 1 3 e は、受注者端末装置 1 1 5 から応答 I n f 3 (本発明の応答) を受信する。

受注者認証部 1 1 3 f は、応答 I n f 3 に含まれる受注者 3 3 の識別情報である個人キー情報 k 2 を用いて受注者 3 3 の認証を行い、認証情報 A u 2 (本発明の第 2 の識別情報) を生成する。

認証応答生成部 1 1 3 g は、応答 I n f 3 に認証情報 A u 2 を付加して認証応答 I n f 4 を生成する。

認証応答暗号化部 1 1 3 h は、認証応答 I n f 4 を暗号化する。

認証応答送信部 1 1 3 i は、暗号化された認証応答 I n f 4 を発注者端末装置 1 1 1 に送信する。

要求暗号化部 1 1 3 j は、要求生成部 1 1 3 c が生成した要求 I n f 2 を暗号化する。

応答復号部 1 1 3 k は、応答 I n f 3 を復号する。

認証要求復号部 1 1 3 l は、認証要求 I n f 1 を復号する。

〔受注者端末装置 1 1 5〕

図 4 は、受注者端末装置 1 1 5 の機能ブロック図である。

受注者端末装置 1 1 5 は、本システム利用の契約を行った商品販売業者等である商品の受注者 3 3 が使用する。

受注者端末装置 1 1 5 は、要求受信部 1 1 5 a、要求復号部 1 1 5 b、応答入力部 1 1 5 c、応答生成部 1 1 5 d、応答暗号化部 1 1 5 e および応答送信部 1

15fを有する。

要求受信部115aは、認証装置113から要求Inf2を受信する。

要求復号部115bは、要求Inf2を復号する。

応答入力部115cは、ユーザによる操作に応じて、受注確認情報C1および受注者33を特定する情報Zを入力する。

応答生成部115dは、要求Inf2、受注確認情報C1および受注者33を特定する情報Zを含む応答Inf3を生成する。

応答暗号化部115eは、応答Inf3を暗号化する。

応答送信部115fは、暗号化された応答Inf3を認証装置113に送信する。

本実施形態のトランザクション認証システム101では、電子商取引の当事者である発注者31と受注者33との間に、その商取引の第三者であるネットワーク銀行121（あるいはトランザクション認証局）が介在し、ネットワーク銀行121が当事者間で行われる電子商取引を認証装置113を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム101の利用を希望する商取引当事者は、まず、このネットワーク銀行121との間で認証装置13の利用契約を結ぶ。

例えば、図1に示すように、発注者31は、インターネット、郵便等を用い、ネットワーク銀行（トランザクション認証局運営会社）21に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者31の氏名、住所等の他、代金等の落とし先となる発注者31が契約している引き落とし銀行42の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行121は、契約を行った発注者31に対し、銀行42からの代金引き落としの際にその正当性を証明する個人ID情報、および本システムにおいて発注者31を識別するための個人キー情報の発行を行う。ここで発行された個人ID情報は銀行42に対しても送られ、銀行42は、商品等の代金引き落としの際にこの個人ID情

報を認証し、代金の不正引き落としを防止する。

なお、図 1 では、発注者 3 1 が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者 3 3 も同様な手順によりネットワーク銀行 1 2 1 との利用契約を結ぶ。また、ここでは、個人 I D 情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人 I D 情報としても利用できることとし、別個の個人 I D 情報を発行しない形態としてもよい。

次に、トランザクション認証システム 1 0 1 の動作について説明する。

ステップ S T 1 1 :

電子商取引によって商品を購入しようとする発注者 3 1 は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者 3 1 は、次に、発注者 3 1 が所有する図 2 に示す発注者端末装置 1 1 1 を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部 1 1 1 a を用い、購入を希望する商品・数量等を指定する発注情報 a 1 および発注者 3 1 の個人キー情報である発注者個人キー情報 k 1 を入力することにより行う。ここで、発注者個人キー情報 k 1 の入力は、発注処理を行うたびに発注者 3 1 が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

これにより、入力された発注情報 a 1 および発注者個人キー情報 k 1 を含む認証要求 I n f 1 が生成され、当該認証要求 I n f 1 が認証要求暗号化部 1 1 1 d で暗号化された後、認証要求送信部 1 1 1 b を介して認証装置 1 1 3 に送信される。

このとき、認証要求送信部 1 1 1 b は、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求 I n f 1 の送信を禁止する不正送信防止機能を有しており、この状態では認証要求 I n f 1 の送信は行われない。

そのため、電子商取引を行おうとする発注者 3 1 は、生体認証装置 1 2 を用い

、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置 1 2 が発注者 3 1 の指紋によって発注者 3 1 を認証するものであった場合、発注者 3 1 は、生体認証装置 1 2 に自己の指紋を読み取らせ、発注者 3 1 の指紋を読み取った生体認証装置 1 2 は、読み取った指紋と、事前
に取得し、内部に格納しておいた発注者 3 1 本人の指紋データとを照合し、読み取った指紋が発注者 3 1 本人のものであるか否か判断する。

そして、読み取った指紋が発注者 3 1 本人のものであると判断された場合、生体認証装置 1 2 は、認証が成立した旨の情報を認証要求送信部 1 1 1 b に指示を与え、この情報を受けた認証要求送信部 1 1 1 b は、不正送信防止機能を解除し、送られた認証要求をトランザクション認証局 3 2 所有の認証装置 1 1 3 に送信する。

ステップ S T 1 2 :

図 3 に示す認証装置 1 1 3 に送信された認証要求 I n f 1 は、認証要求受信部 1 1 3 a で受信され、認証要求復号部 1 1 3 1 によって復号された後、発注者認証部 1 1 3 b に送られる。

次に、発注者認証部 1 1 3 b において、認証要求 I n f 1 に含まれる発注者個人キー情報 k 1 と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者 3 1 であるか否かが判断される。

そして、正当な発注者 3 1 であると判断されると、認証要求 I n f 1 は要求生成部 1 1 3 c に送られて、要求生成部 1 1 3 c において、認証要求 I n f 1 から個人キー情報 k 1 を削除して生成された情報 I n f 1 a と、認証情報 A u 1 とを含む要求 I n f 2 (本発明の第 2 の要求) が生成される。

当該 I n f 2 は、要求暗号化部 1 1 3 j において暗号化された後に、要求送信部 1 1 3 d を介して受注者端末装置 1 1 5 に送信される。

また、認証要求 I n f 1 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

ステップ S T 1 3 :

受注者端末装置 1 1 5 に送信された要求 I n f 2 は、要求受信部 1 1 5 a によって受信された後、要求復号部 1 1 5 b により復号され、受注者 3 3 は、復号された要求 I n f 2 に基づいて商品の受注処理を行う。

受注処理は、受注者 3 3 が応答入力部 1 1 5 c を用い、受注確認情報 C 1 および受注者 3 3 を特定する情報 Z を入力することにより行われる。ここで、情報 Z の入力は、受注処理を行うたびに受注者 3 3 が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

次に、応答生成部 1 1 5 d において、要求 I n f 2、受注確認情報 C 1 および情報 Z を含む応答 I n f 3 が生成され、当該応答 I n f 3 が、応答暗号化部 1 1 5 e で暗号化された後に、応答送信部 1 1 5 f を介して認証装置 1 1 3 に送信される。

ステップ S T 1 4 :

認証装置 1 1 3 に送信された応答 I n f 3 は、図 3 に示す応答受信部 1 1 3 e で受信され、応答復号部 1 1 3 k によって復号された後、受注者認証部 1 1 3 f に送られる。

次に、受注者認証部 1 1 3 f において、応答 I n f 3 に含まれる情報 Z と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者 3 3 であるか否かが判断される。

そして、正当な受注者 3 3 であると判断されると、応答 I n f 3 は認証応答生成部 1 1 3 g に送られて、認証応答生成部 1 1 3 g において、応答 I n f 3 と、認証が成立したことを示す認証情報 A u 2 とを含む認証応答 I n f 4 が生成される。

当該認証応答 I n f 4 は、認証応答暗号化部 1 1 3 h において暗号化された後に、認証応答送信部 1 1 3 i を介して発注者端末装置 1 1 1 に送信される。

また、応答 I n f 3 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

発注者端末装置 1 1 1 に送信された認証応答 I n f 4 は、図 2 に示す認証応答受信部 1 1 1 c で受信された後、認証応答復号手投 1 1 e によって復号され、発注者 3 1 は、この復号された認証応答 I n f 4 を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。

その後、ネットワーク銀行 2 1 は、発注者 3 1 の個人キー情報 k 1 を用いて、発注者 3 1 が契約する引き落とし銀行 4 2 の銀行口座から、当該取り引きに伴う金額を引き落とす。当該引き落としは、ネットワーク銀行 2 1 の銀行口座に引き落としてから受注者 3 3 の銀行口座に振り込んでもよいし、発注者 3 1 の銀行口座から受注者 3 3 の銀行口座に振り込みを直接行ってもよい。

また、受注者 3 3 は、発注情報 a 1 に基づいて、発注者 3 1 に商品およびサービスを提供する。

以上説明したように、トランザクション認証システム 1 0 1 によれば、発注者端末装置 1 1 1 および受注者端末装置 1 1 5 を用いた、発注者 3 1 と受注者 3 3 との間の電子商取引を認証装置 1 1 3 を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム 1 0 1 によれば、認証装置 1 1 3 から受注者端末装置 1 1 5 に送信される要求 I n f 2 には、受注者 3 3 の個人キー情報 k 1 を含まないため、発注者 3 1 の課金に係わる個人キー情報が受注者 3 3 に渡ることはない。そのため、個人キー情報の不正利用を効果的に抑制できる。

また、トランザクション認証システム 1 0 1 によれば、第三者が発注者個人キー情報 k 1 を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答 I n f 4 は正規の発注者 3 1 に送信されることとなり、正規の発注者 3 1 は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

また、認証装置 1 1 3 によって、認証要求 I n f 1 および応答 I n f 3 を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

さらに、認証履歴格納装置 1 4 によって、認証要求 I n f 1 および応答 I n f 3 を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

また、認証要求 I n f 1、要求 I n f 2、応答 I n f 3 および認証応答 I n f 4 は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

さらに、認証要求送信部 1 1 1 b は、生体認証装置 1 2 によって発注者 3 1 が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

第 2 実施形態

図 6 は、本実施形態におけるトランザクション認証システム 1 の構成を示した構成図である。

トランザクション認証システム 1 は、発注者 3 1 が発注処理を行う発注者端末装置 1 1 と、発注者 3 1 の生体的特徴を利用して発注者 3 1 が本人であることを認証する生体認証装置 1 2 と、ネットワーク銀行（あるいはトランザクション認証局運営会社） 2 1 によって使用され、商取引情報の認証を行う認証装置 1 3 と、認証履歴を格納する認証履歴格納装置 1 4 と、受注者 3 3 が受注処理を行う受注者端末装置 1 5 とを有する。

本実施形態は、第 4 ～ 6 発明に対応した実施形態であり、発注者端末装置 1 1 が本発明の第 1 の通信装置に対応し、認証装置 1 3 が本発明の認証装置に対応し、受注者端末装置 1 5 が本発明の第 2 の通信装置に対応している。また、発注者

3 1 が本発明の第 1 の取り引き者に対応し、受注者 3 3 が本発明の第 2 の取り引き者に対応している。

〔発注者端末装置 1 1〕

図 7 は、発注者端末装置 1 1 の機能ブロック図である。

発注者端末装置 1 1 は、本システム利用の契約を行った一般利用者である発注者 3 1 が使用する端末装置である。

発注者端末装置 1 1 は、図 7 に示すように、認証要求入力部 1 1 a、認証要求送信部 1 1 b、認証応答受信部 1 1 c、認証要求暗号化部 1 1 d および認証応答復号部 1 1 e を有する。

認証要求入力部 1 1 a は、例えば、発注者 3 1 によるキーボードなどの操作に応じて、発注情報 a 1、発注者個人 ID 情報 ID 1（本発明の第 1 の取り引き者の個人識別情報）および発注者個人キー情報 k 1（本発明の第 1 の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報 a 1 には、例えば、発注者 3 1 の名前、住所、連絡先、受注者 3 3 の個人 ID 情報 ID 2（本発明の第 2 の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部 1 1 b は、認証要求入力部 1 1 a に入力された発注情報 a 1、発注者個人 ID 情報 ID 1 および発注者個人キー情報を含む認証要求 Inf 1（本発明の第 1 の要求）を認証装置 1 3 に送信する。

認証応答受信部 1 1 c は、認証装置 1 3 から認証応答 Inf 4 を受信する。

認証要求暗号化部 1 1 d は、認証要求 Inf 1 を暗号化する。

認証応答復号部 1 1 e は、認証応答 Inf 4 を復号する。

生体認証装置 1 2 は、いわゆるバイオメトリックス (biometrics) を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置 1 2 に格納しておいた利用者（発注者 3 1）の指紋等の身体的特徴と、実際に認証

を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置 1 2 の記録装置は、外部から電氣的に切断されており、その情報が外部に流出しない構成となっている。

〔認証装置 1 3〕

図 8 は、認証装置 1 3 の機能ブロック図である。

認証装置 1 3 は、本システムを運営するネットワーク銀行 2 1 が使用する装置である。

認証装置 1 3 は、図 8 に示すように、認証要求受信部 1 3 a、発注者認証部 1 3 b、要求生成部 1 3 c、要求送信部 1 3 d、応答受信部 1 3 e、受注者認証部 1 3 f、認証応答生成部 1 3 g、認証応答暗号化部 1 3 h、認証応答送信部 1 3 i、要求暗号化部 1 3 j、応答復号部 1 3 k および認証要求復号部 1 3 l を有する。

ここで、認証要求受信部 1 3 a が本発明の第 1 の受信手段に対応し、発注者認証部 1 3 b および要求生成部 1 3 c が本発明の第 1 の認証手段に対応し、要求送信部 1 3 d が本発明の第 1 の送信手段に対応し、応答受信部 1 3 e が本発明の第 2 の受信手段に対応し、受注者認証部 1 3 f および認証応答生成部 1 3 g が本発明の第 2 の認証手段に対応し、認証応答暗号化部 1 3 h が本発明の暗号化手段に対応し、認証応答送信部 1 3 i が本発明の第 2 の送信手段に対応し、要求暗号化部 1 3 j が本発明の暗号化手段に対応し、応答復号部 1 3 k が本発明の復号手段に対応し、認証要求復号部 1 3 l が本発明の復号手段に対応している。

認証要求受信部 1 3 a は、発注者端末装置 1 1 が送信した認証要求 I n f 1 を受信する。

発注者認証部 1 3 b は、認証要求 I n f 1 が含む発注者個人 I D 情報 I D 1 および発注者個人キー情報 k 1 を用いて発注者 3 1 の認証を行い、認証情報 A u 1 (本発明の第 1 の認証情報) を生成する。

要求生成部 13 c は、発注者認証部 13 b によって認証された認証要求 I n f 1 に認証情報 A u 1 を付加して要求 I n f 2（本発明の第 2 の要求）を生成する。

要求送信部 13 d は、要求 I n f 2 を受注者端末装置 15 に送信する。

応答受信部 13 e は、受注者端末装置 15 から応答 I n f 3（本発明の応答）を受信する。

受注者認証部 13 f は、応答 I n f 3 に含まれる受注者 33 の識別情報である個人キー情報 k 2 を用いて受注者 33 の認証を行い、認証情報 A u 2（本発明の第 2 の識別情報）を生成する。

認証応答生成部 13 g は、応答 I n f 3 に認証情報 A u 2 を付加して認証応答 I n f 4 を生成する。

認証応答暗号化部 13 h は、認証応答 I n f 4 を暗号化する。

認証応答送信部 13 i は、暗号化された認証応答 I n f 4 を発注者端末装置 11 に送信する。

要求暗号化部 13 j は、要求生成部 13 c が生成した要求 I n f 2 を暗号化する。

応答復号部 13 k は、応答 I n f 3 を復号する。

認証要求復号部 13 l は、認証要求 I n f 1 を復号する。

〔受注者端末装置 15〕

図 9 は、受注者端末装置 15 の機能ブロック図である。

受注者端末装置 15 は、本システム利用の契約を行った商品販売業者等である商品の受注者 33 が使用する。

受注者端末装置 15 は、要求受信部 15 a、要求復号部 15 b、応答入力部 15 c、応答生成部 15 d、応答暗号化部 15 e および応答送信部 15 f を有する。

要求受信部 15 a は、認証装置 13 から要求 I n f 2 を受信する。

要求復号部 15 b は、要求 I n f 2 を復号する。

応答入力部 15 c は、ユーザによる操作に応じて、受注確認情報 C 1 および受注者 3 3 を特定する情報 Z を入力する。

応答生成部 15 d は、要求 I n f 2、受注確認情報 C 1 および情報 Z を含む応答 I n f 3 を生成する。

応答暗号化部 15 e は、応答 I n f 3 を暗号化する。

応答送信部 15 f は、暗号化された応答 I n f 3 を認証装置 1 3 に送信する。

本実施形態のトランザクション認証システム 1 では、電子商取引の当事者である発注者 3 1 と受注者 3 3 との間に、その商取引の第三者であるネットワーク銀行 2 1（あるいはトランザクション認証局）が介在し、ネットワーク銀行 2 1 が当事者間で行われる電子商取引を認証装置 1 3 を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム 1 の利用を希望する商取引当事者は、まず、このネットワーク銀行 2 1 との間で認証装置 1 3 の利用契約を結ぶ。

例えば、図 6 に示すように、発注者 3 1 は、インターネット、郵便等を用い、ネットワーク銀行 2 1 に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者 3 1 の氏名、住所等の他、代金等の落とし先となる発注者 3 1 が契約している引き落とし銀行 4 2 の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行 2 1 は、契約を行った発注者 3 1 に対し、銀行 4 2 からの代金引き落としの際にその正当性を証明する個人 I D 情報、および本システムにおいて発注者 3 1 を識別するための個人キー情報の発行を行う。ここで発行された個人 I D 情報は銀行 4 2 に対しても送られ、銀行 4 2 は、商品等の代金引き落としの際にこの個人 I D 情報を認証し、代金の不正引き落としを防止する。

なお、図 6 では、発注者 3 1 が利用契約を結ぶ場合についてのみ説明したが、

商品販売業者等である商品の受注者 3 3 も同様な手順によりネットワーク銀行 2 1 との利用契約を結ぶ。また、ここでは、個人 I D 情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人 I D 情報としても利用できることとし、別個の個人 I D 情報を発行しない形態としてもよい。

次に、トランザクション認証システム 1 の動作について説明する。

ステップ S T 1 :

電子商取引によって商品を購入しようとする発注者 3 1 は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者 3 1 は、次に、発注者 3 1 が所有する図 7 に示す発注者端末装置 1 1 を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部 1 1 a を用い、購入を希望する商品・数量等を指定する発注情報 a 1、契約時に発行された発注者 3 1 の個人 I D 情報である発注者個人 I D 情報 I D 1、および発注者の個人キー情報である発注者個人キー情報 k 1 を入力することにより行う。ここで、発注者個人 I D 情報 I D 1 および発注者個人キー情報 k 1 の入力、発注処理を行うたびに発注者 3 1 が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

これにより、入力された発注情報 a 1、発注者個人 I D 情報 I D 1 および発注者個人キー情報 k 1 を含む認証要求 I n f 1 が生成され、当該認証要求 I n f 1 が認証要求暗号化部 1 1 d で暗号化された後、認証要求送信部 1 1 b を介して認証装置 1 3 に送信される。

このとき、認証要求送信部 1 1 b は、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求 I n f 1 の送信を禁止する不正送信防止機能を有しており、この状態では認証要求 I n f 1 の送信は行われない。

そのため、電子商取引を行おうとする発注者 3 1 は、生体認証装置 1 2 を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置 1 2 が発注者 3 1 の指紋によって発注者 3 1 を認証するものであった場合、発注者 3 1 は、生体認証装置 1 2 に自己の指紋を読み取らせ、発注者 3 1 の指紋を読み取った生体認証装置 1 2 は、読み取った指紋と、事前に取得し、内部に格納しておいた発注者 3 1 本人の指紋データとを照合し、読み取った指紋が発注者 3 1 本人のものであるか否か判断する。

そして、読み取った指紋が発注者 3 1 本人のものであると判断された場合、生体認証装置 1 2 は、認証が成立した旨の情報を認証要求送信部 1 1 b に指示を与え、この情報を受けた認証要求送信部 1 1 b は、不正送信防止機能を解除し、送られた認証要求をネットワーク銀行 2 1 所有の認証装置 1 3 に送信する。

ステップ S T 2 :

図 8 に示す認証装置 1 3 に送信された認証要求 I n f 1 は、認証要求受信部 1 3 a で受信され、認証要求復号部 1 3 1 によって復号された後、発注者認証部 1 3 b に送られる。

次に、発注者認証部 1 3 b において、認証要求 I n f 1 に含まれる発注者個人 I D 情報 I D 1 と、発注者個人キー情報 k 1 と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者 3 1 であるか否かが判断される。

そして、正当な発注者 3 1 であると判断されると、認証要求 I n f 1 は要求生成部 1 3 c に送られて、要求生成部 1 3 c において、認証要求 I n f 1 と、認証が成立したことを示す認証情報 A u 1 とを含む要求 I n f 2 が生成される。

当該 I n f 2 は、要求暗号化部 1 3 j において暗号化された後に、要求送信部 1 3 d を介して受注者端末装置 1 5 に送信される。

また、認証要求 I n f 1 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

ステップ S T 3 :

受注者端末装置 1 5 に送信された要求 I n f 2 は、要求受信部 1 5 a によって

受信された後、要求復号部 1 5 b により復号され、受注者 3 3 は、復号された要求 I n f 2 に基づいて商品の受注処理を行う。

受注処理は、受注者 3 3 が応答入力部 1 5 c を用い、受注確認情報 C 1 および受注者 3 3 を特定する情報 Z を入力することにより行われる。ここで、当該情報 Z の入力、受注処理を行うたびに受注者 3 3 が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

次に、応答生成部 1 5 d において、要求 I n f 2、受注確認情報 C 1 および受注者 3 3 を特定する情報 Z を含む応答 I n f 3 が生成され、当該応答 I n f 3 が、応答暗号化部 1 5 e で暗号化された後に、応答送信部 1 5 f を介して認証装置 1 3 に送信される。

ステップ S T 4 :

認証装置 1 3 に送信された応答 I n f 3 は、図 8 に示す応答受信部 1 3 e で受信され、応答復号部 1 3 k によって復号された後、受注者認証部 1 3 f に送られる。

次に、受注者認証部 1 3 f において、応答 I n f 3 に含まれる情報 Z と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者 3 3 であるか否かが判断される。

そして、正当な受注者 3 3 であると判断されると、応答 I n f 3 は認証応答生成部 1 3 g に送られて、認証応答生成部 1 3 g において、応答 I n f 3 と、認証が成立したことを示す認証情報 A u 2 とを含む認証応答 I n f 4 が生成される。

当該認証応答 I n f 4 は、認証応答暗号化部 1 3 h において暗号化された後に、認証応答送信部 1 3 i を介して発注者端末装置 1 1 に送信される。

また、応答 I n f 3 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

発注者端末装置 1 1 に送信された認証応答 I n f 4 は、図 7 に示す認証応答受

信部 1 1 c で受信された後、認証応答復号手投 1 1 e によって復号され、発注者 3 1 は、この復号された認証応答 I n f 4 を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。その後、受注者 3 3 は、発注者 3 1 の発注者個人 I D 情報 I D 1 を用い、発注者 3 1 が契約している銀行から、発注を受けた商品代金の引き落としを行い、さらに、発注を受けた商品を発注者 3 1 に郵送する。

以上説明したように、トランザクション認証システム 1 によれば、発注者端末装置 1 1 および受注者端末装置 1 5 を用いた、発注者 3 1 と受注者 3 3 との間の電子商取引を認証装置 1 3 を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム 1 によれば、第三者が発注者個人キー情報 k 1 を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答 I n f 4 は正規の発注者 3 1 に送信されることとなり、正規の発注者 3 1 は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

また、認証装置 1 3 によって、認証要求 I n f 1 および応答 I n f 3 を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

さらに、認証履歴格納装置 1 4 によって、認証要求 I n f 1 および応答 I n f 3 を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

また、認証要求 I n f 1、要求 I n f 2、応答 I n f 3 および認証応答 I n f 4 は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

さらに、認証要求送信部 1 1 b は、生体認証装置 1 2 によって発注者 3 1 が本

人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、発注者端末装置 11、認証装置 13、受注者端末装置 15 が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場に流通させる場合には、CD-ROM (Compact Disc Read Only Memory) やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

なお、本形態では、トランザクション認証システム 1 を、電子商取引において利用することとしたが、電子通信回線を用いたアンケート、投票、その他情報伝送時における不正防止のために利用することとしてもよい。

また、上述した実施形態では、発注者端末装置 11 から認証装置 13 に、発注者個人 ID 情報 ID 1 を含む認証要求 Inf 1 を送信する場合を例示したが、発注者個人 ID 情報 ID 1 を含まない認証要求 Inf 1 を送信してもよい。

第 3 実施形態

図 11 は、本実施形態のトランザクション認証システム 301 の全体構成図である。

図 11 に示すように、トランザクション認証システム 301 では、例えば、発注者 31 の発注者端末装置 311 と、受注者 33 の受注者端末装置 315 と、ネ

ネットワーク銀行 340 の認証装置 350 と、ネットワーク銀行 341 の認証装置 351 と、認証履歴を格納する認証履歴格納装置 14 とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者 31 と受注者 33 との間のトランザクション（取引）の正当性を認証する。

本実施形態では、例えば、発注者 31 とネットワーク銀行 340 との間で認証を行うことに関する契約が成されており、受注者 33 とネットワーク銀行 341 との間で認証を行うことに関する契約が成されている。

また、ネットワーク銀行 340 とネットワーク銀行 341 とでは、認証に関して、相互に連携する旨の相互乗り入れの契約が成立されている。

本実施形態は、第 7 ～ 9 の発明に対応した実施形態である。

本実施形態では、発注者 31 が本発明の第 1 の取引引き者に対応し、受注者 33 が本発明の第 2 の取引引き者に対応している。

また、認証装置 350 が、第 7 の発明の認証装置、並びに第 8 の発明および第 9 の発明の第 1 の認証装置に対応している。

また、認証装置 351 が、第 7 の発明の他の認証装置、並びに第 8 の発明および第 9 の発明の第 2 の認証装置に対応している。

以下、トランザクション認証システム 301 を構成する各装置について説明する。

〔発注者端末装置 311〕

図 12 に示すように、発注者端末装置 311 は、例えば、発注者 31 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 361、送信部 362、暗号化部 363、復号部 364、記憶部 365、制御部 366 および署名検証部 367 を有する。

なお、発注者端末装置 311 は、例えば、発注者 31 が使用する際に、発注者 31 の指紋等の身体的特徴から得られる情報と、予め記憶部 365 に予め記憶し

である身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な使用者であることを認証する生態認証部を有していてもよい。

受信部 3 6 1 は、ネットワークを介して認証装置 3 5 0 から情報あるいは要求を受信する。

送信部 3 6 2 は、ネットワークを介して認証装置 3 5 0 に情報あるいは要求を送信する。

また、受信部 3 6 1 および送信部 3 6 2 は、受注者 3 3 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 3 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 3 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 3 6 5 は、例えば、発注者 3 1 がネットワーク銀行 3 4 0 と契約を行うと、例えば、発注者 3 1 に割り当てられた秘密鍵 $K_{31, s}$ などを格納する。

制御部 3 6 6 は、発注者端末装置 3 1 1 内の各構成要素の処理を統括的に制御する。

署名検証部 3 6 7 は、例えば、認証装置 3 5 0 が作成した署名情報を、ネットワーク銀行 3 4 0 の公開鍵 $K_{40, p}$ を用いて検証する。

〔受注者端末装置 3 1 5〕

図 1 3 に示すように、受注者端末装置 3 1 5 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 3 7 1、送信部 3 7 2、暗号化部 3 7 3、復号部 3 7 4、記憶部 3 7 5、制御部 3 7 6 および署名検証部 3 7 7 を有する。

受信部 3 7 1 は、ネットワークを介して認証装置 3 5 0, 3 5 1 から情報あるいは要求を受信する。

送信部 3 7 2 は、ネットワークを介して認証装置 3 5 0, 3 5 1 に情報あるいは

は要求を送信する。

また、受信部 371 および送信部 372 は、発注者端末装置 311 からのアクセスに応じて、例えば、記憶部 375 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 311 に送信する。

暗号化部 373 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 374 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 375 は、例えば、受注者 33 がネットワーク銀行 341 と契約を行うと、例えば、受注者 33 に割り当てられた秘密鍵 $K_{33, s}$ などを格納する。

制御部 376 は、受注者端末装置 315 内の各構成要素の処理を統括的に制御する。

署名検証部 377 は、例えば、受注者 33 の公開鍵 $K_{33, p}$ を用いて、受注者端末装置 315 が作成した署名情報の検証を行う。

〔認証装置 350〕

図 14 に示すように、認証装置 350 は、受信部 381、送信部 382、暗号化部 383、復号部 384、記憶部 385、制御部 386、署名作成部 387 および課金処理部 388 を有する。

ここで、受信部 381 および送信部 382 が、第 7 の発明の送受信手段に対応し、記憶部 385 が第 7 の発明の記憶手段に対応し、署名作成部 387 が第 7 の発明の署名作成手段に対応している。

受信部 381 は、ネットワークを介して発注者端末装置 311、受注者端末装置 315 および認証装置 351 から情報あるいは要求を受信する。

送信部 382 は、ネットワークを介して発注者端末装置 311、受注者端末装置 315 および認証装置 351 に情報あるいは要求を送信する。

暗号化部 383 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 384 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 385 は、例えば、発注者 31 がネットワーク銀行 340 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵 $K_{31, s}$ に対応する公開鍵 $K_{33, p}$ などを格納する。

制御部 386 は、認証装置 350 内の各構成要素の処理を統括的に制御する。

署名作成部 387 は、ネットワーク銀行 340 の秘密鍵 $K_{40, s}$ を用いて署名情報の作成を行う。

課金処理部 388 は、発注者 31 による取引に関する認証に対しての課金処理を行い、認証装置 351 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

認証装置 350 の各構成要素の詳細な処理については、後述する動作例で記載する。

〔認証装置 351〕

図 15 に示すように、認証装置 351 は、受信部 391、送信部 392、暗号化部 393、復号部 394、記憶部 395、制御部 396、署名作成部 397 および課金処理部 398 を有する。

受信部 391 は、ネットワークを介して受注者端末装置 315 および認証装置 350 から情報あるいは要求を受信する。

送信部 392 は、ネットワークを介して受注者端末装置 315 および認証装置 350 に情報あるいは要求を送信する。

暗号化部 393 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 394 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 395 は、受注者 33 がネットワーク銀行 341 と契約を行うと、例えば、受注者 33 に割り当てられた秘密鍵 $K_{33, s}$ に対応する公開鍵 $K_{33, p}$ などを格

納する。

制御部 396 は、認証装置 351 内の各構成要素の処理を統括的に制御する。

署名作成部 397 は、ネットワーク銀行 341 の秘密鍵 $K_{41,s}$ を用いて署名情報の作成を行う。

課金処理部 398 は、受注者 33 による取引に関する認証に対しての課金処理を行い、認証装置 350 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

以下、トランザクション認証システム 301 の動作例を説明する。

以下に示す動作例を開始する前提として、発注者 31 とネットワーク銀行 340 との間で所定の契約が結ばれ、ネットワーク銀行 340 は、発注者 31 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行する。ネットワーク銀行 340 は、個人キー情報 k_1 および個人 ID 情報 ID_1 の対応表を図 14 に示す認証装置 350 の記憶部 385 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 340 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行 340 は、自らの秘密鍵 $K_{40,s}$ を図 14 に示す認証装置 350 の記憶部 385 に記憶すると共に、当該秘密鍵 $K_{40,s}$ に対応する公開鍵 $K_{40,p}$ を発注者端末装置 311 に送信する。発注者端末装置 311 は、公開鍵 $K_{40,p}$ を図 12 に示す記憶部 365 に記憶する。

また、受注者 33 とネットワーク銀行 341 との間で所定の契約が結ばれ、ネットワーク銀行 341 は、受注者 33 に対して、受注者 33 を特定する情報 Z および個人 ID 情報 ID_2 を発行する。ネットワーク銀行 341 は、情報 Z および個人 ID 情報 ID_2 の対応表を図 15 に示す認証装置 351 の記憶部 395 に記憶する。

また、ネットワーク銀行 341 は、自らの秘密鍵 $K_{41,s}$ を図 15 に示す認証装置 351 の記憶部 395 に記憶すると共に、当該秘密鍵 $K_{41,s}$ に対応する公開鍵 $K_{41,p}$ を受注者端末装置 315 に送信する。受注者端末装置 315 は、公開鍵 $K_{41,p}$ を図 13 に示す記憶部 375 に記憶する。

また、ネットワーク銀行 340 とネットワーク銀行 341 との間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置 350 と認証装置 351 との間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

図 16A～16F は、トランザクション認証システム 301 の動作例を説明するための図である。

ステップ ST31 :

発注者端末装置 311 は、図 11 に示す発注者 31 は、例えばネットワーク上の商店である受注者 33 に商品を発注する場合に、受注者 33 を特定する情報（例えば受注者 33 の名前）、発注する商品名および数量などを示す発注情報 $a1$ と、発注者 31 の個人キー情報 $k1$ と、発注者 31 の個人 ID 情報 $ID1$ とを、図示しない操作手段を操作して発注者端末装置 311 に入力する。なお、発注情報 $a1$ には、受注者 33 を特定する情報が含まれている。

次に、図 12 に示す発注者端末装置 311 の暗号化部 363 は、記憶部 365 から読み出した所定の暗号鍵を用いて、発注情報 $a1$ と、個人キー情報 $k1$ および個人 ID 情報 $ID1$ を暗号化し、当該暗号化した情報を格納した認証要求 $Inf1$ （本発明の第 1 の要求）を、送信部 362 からネットワークを介して、図 11 に示すネットワーク銀行 340 に送信する。

ステップ ST32 :

図 14 に示す認証装置 350 は、発注者端末装置 311 からの認証要求 $Inf1$ を受信部 381 が受信すると、記憶部 385 から所定の暗号化鍵を読み出し、復号部 384 において、当該暗号鍵を用いて認証要求 $Inf1$ を復号する。

次に、認証装置 350 は、制御部 386 の制御に基づいて、上記復号した認証要求 Inf 1 に格納された発注情報 a 1 に含まれる受注者 33 を特定する情報 b 1 を格納した要求 Inf 2（本発明の第 2 の要求）を、記憶部 385 から読み出した所定の暗号鍵を用いて暗号化部 383 で暗号化した後に、受信部 381 からネットワークを介して認証装置 351 に送信する。

ステップ S T 3 3 :

図 15 に示す認証装置 351 の制御部 396 は、認証装置 350 からの要求 Inf 2 を受信部 391 が受信すると、記憶部 395 から読み出した所定の暗号鍵を用いて復号部 394 において当該要求 Inf 2 を復号する。

次に、署名作成部 397 は、当該復号された要求 Inf 2 に格納された受注者 33 を特定する情報 b 1 に対応する受注者 33 の公開鍵 $K_{33, P}$ を記憶部 385 から読み出し、当該公開鍵 $K_{33, P}$ について、記憶部 385 から読み出した自らの秘密鍵 $K_{41, S}$ を用いて自らの認証結果を示す署名情報 A u - B（本発明の第 1 の署名情報）を作成する。

次に、暗号化部 393 は、受注者 33 の公開鍵 $K_{33, P}$ および署名情報 A u - B を格納した応答 Inf 3 を、記憶部 395 から読み出した所定の暗号鍵を用いて暗号化した後に、送信部 392 からネットワークを介して認証装置 350 に送信する。

ステップ S T 3 4 :

図 14 に示す認証装置 350 の復号部 384 は、認証装置 351 からの応答 Inf 3 を受信部 381 が受信すると、記憶部 385 から読み出した所定の暗号鍵を用いて、応答 Inf 3 を復号する。

次に、署名作成部 387 は、ステップ S T 3 2 で復号した要求 Inf 1 から個人キー情報 k 1 および個人 ID 情報 ID 1 を削除した情報 Inf 1' と、上記復号された応答 Inf 3 に格納された署名情報 A u - B と、記憶部 385 から読み出した自らの公開鍵 $K_{40, P}$ について、記憶部 385 から読み出した自らの秘密

鍵 $K_{40,s}$ を用いて署名情報 $A_u - A_1$ を作成する。

次に、制御部 386 は、情報 $I_{nf1'}$ と、署名情報 $A_u - B$ と、自らの公開鍵 $K_{40,p}$ と、上記生成した署名情報 $A_u - A_1$ とを格納した要求 I_{nf4} （本発明の第 3 の要求）を生成する。

次に、暗号化部 383 は、ステップ ST34 で認証装置 351 から受信した受注者 33 の公開鍵 $K_{33,p}$ を用いて、上記生成した要求 I_{nf4} を暗号化した後に、送信部 382 から、ネットワークを介して受注者端末装置 315 に送信する。

ステップ ST35 :

受注者端末装置 315 の復号部 374 は、認証装置 350 からの要求 I_{nf4} を受信部 371 が受信すると、記憶部 375 から読み出した自らの秘密鍵 $K_{33,s}$ を用いて、要求 I_{nf4} を復号する。

次に、受注者端末装置 315 の署名検証部 377 は、上記復号した要求 I_{nf4} に格納された署名情報 $A_u - B$ を、記憶部 375 から読み出した認証装置 351 の公開鍵 $K_{41,p}$ を用いて検証する。また、署名情報検証部は、上記復号した要求 I_{nf4} に格納された認証装置 350 の公開鍵 $K_{40,p}$ を用いて、要求 I_{nf4} に格納された署名情報 $A_u - A_1$ を検証する。

受注者端末装置 315 の制御部 376 は、署名検証部が上記検証の結果、署名情報 $A_u - B$ 、 $A_u - A_1$ の正当性が認証されると、要求 I_{nf4} に格納された情報 $I_{nf1'}$ と、署名情報 $A_u - B$ 、 $A_u - A_1$ と、受注者 33 を特定する情報 Z とを格納した応答 I_{nf5} （本発明の所定の応答）を生成する。

次に、受注者端末装置 315 の送信部 372 は、上記生成した応答 I_{nf5} を、上記復号した要求 I_{nf4} に格納された認証装置 350 の公開鍵 $K_{40,p}$ を用いて復号した後に、送信部 372 から、ネットワークを介して認証装置 350 に送信する。

受注者端末装置 315 によって、署名情報 $A_u - B$ 、 $A_u - A_1$ の正当性が認

証されると、受注者 33 は、例えば、要求 Inf 4 に格納された情報 Inf 1' 内の発注情報 a 1 に基づいて、発注者 31 が発注した商品等を発注者 31 に発送したり、発注者 31 が注文したサービスを発注者 31 に提供する。

ステップ ST 36 :

認証装置 350 の復号部 384 は、受注者端末装置 315 からの応答 Inf 5 を受信部 381 が受信すると、記憶部 385 から読み出した自らの秘密鍵 $K_{40,s}$ を用いて、Inf 5 を復号し、要求 Inf 1 に格納された発注情報 a 1 と、当該復号された Inf 5 に格納された受注者 33 を特定する情報 Z とを用いて、所定の取引履歴情報を作成し、これを記憶部 385 に格納する。当該履歴情報は、ネットワーク銀行 340 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 350 の署名作成部 387 は、ステップ ST 32 で受信した要求 Inf 1 と、応答 Inf 5 に含まれる情報 Z と、ステップ ST 34 で作成した署名情報 Au-A 1 とについて、自らの秘密鍵 $K_{40,s}$ を用いて自らの認証結果を示す署名情報 Au-A 2 (本発明の第 2 の署名情報) を作成する。

次に、認証装置 350 の制御部 386 は、要求 Inf 1 と、情報 Z と、署名情報 Au-A 1 と、署名情報 Au-A 2 とを格納した応答 Inf 6 を作成する。

次に、認証装置 350 の暗号化部 383 は、上記作成した応答 Inf 6 を、認証装置 350 から読み出した所定の暗号鍵を用いて暗号化した後に、送信部 382 から、ネットワークを介して発注者端末装置 311 に送信する。

発注者端末装置 311 では、受信した応答 Inf 6 を、図 12 に示す記憶部 365 から読み出した所定の暗号鍵を用いて復号部 364 で復号する。

次に、発注者端末装置 311 の署名検証部 366 は、当該復号した応答 Inf 6 に格納された署名情報 Au-A 1, Au-A 2 を、記憶部 365 から読み出したネットワーク銀行 340 の公開鍵 $K_{40,P}$ を用いて検証することで、受注者端末装置 315 との間の当該取引が正当に認証されたことを確認する。

以上説明したように、トランザクション認証システム 301 によれば、認証装置 350 から認証装置 351 へは、発注者 31 の個人キー情報 k_1 および個人 ID 情報 ID_1 を送信しないことから、発注者 31 の個人情報、発注者 31 が契約していない他のネットワーク銀行 341 に漏れることを回避できる。

また、トランザクション認証システム 301 によれば、認証装置 350 が、認証装置 351 から受けた受注者 33 の公開鍵 $K_{33, P}$ および署名情報 A_{u-B} を用いて、受注者 33 の受注者端末装置 315 との間で直接通信を行うことで、当該取り引きの履歴を認証装置 350 に格納できる。

また、トランザクション認証システム 301 によれば、受注者 33 は、自らの契約した認証装置 350 の署名情報 A_{u-B} を検証することで、当該取り引きの正当性を確認できる。

また、トランザクション認証システム 301 によれば、認証装置 350 と 351 との間では、図 16A~16F に示す要求 Inf_2 および Inf_3 を伝送するだけで、発注者 31 と受注者 33 との間の取り引きを認証でき、認証装置 350 と 351 との間の通信量を小さくできる。

また、トランザクション認証システム 301 によれば、図 14 に示す認証装置 350 の課金処理部 388 と、図 15 に示す認証装置 351 の課金処理部 398 との間で通信を行うことで、発注者 31 と受注者 33 との間の取り引きに関する認証に対して行う課金の割合を柔軟に決定できる。

上述したように、トランザクション認証システム 301 によれば、異なる認証機関と契約をしている複数の取り引き者の間の取り引きに関する認証を、高い信頼性で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行 340, 341 が、それぞ

れ認証装置 350, 351 を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行 340, 341 とは別の機関が、認証装置 350, 351 を用いてトランザクションの認証業務を行うようにしてもよい。

また、上述した実施形態では、発注者 31 が契約したネットワーク銀行 340 の認証装置 350 と、受注者 33 が契約したネットワーク銀行 341 の認証装置 351 との間で連携して認証処理を行う場合を例示したが、3 人以上の取引者がそれぞれ異なる認証機関と契約を行っている場合に、3 以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

また、上述した実施形態では、図 16 A に示すステップ S T 31 のように、暗号化された発注情報 a 1 と、個人キー情報 k 1 および個人 ID 情報 I D 1 とを含む認証要求 I n f 1 を、発注者端末装置 311 から認証装置 350 に送信する場合を例示したが、発注情報 a 1 および個人キー情報 k 1 を含む認証要求 I n f 1 を、発注者端末装置 311 から認証装置 350 に送信してもよい。このようにすれば、課金に係わる情報である個人 ID 情報 I D 1 はネットワークを介して伝送されないため、ネットワーク上で個人 ID 情報 I D 1 が不正に取得され、悪用されることを回避できる。

また、本発明では、例えば、認証装置 350 から受注者端末装置 315 に、署名情報 A u - A 2（本発明の第 2 の署名情報）を送信するようにしてもよい。

第 4 実施形態

図 17 は、本実施形態のトランザクション認証システム 1301 の全体構成図である。

図 17 に示すように、トランザクション認証システム 1301 では、例えば、発注者 31 の発注者端末装置 1311 と、受注者 33 の受注者端末装置 1315 と、ネットワーク銀行 1340 の認証装置 1350 と、ネットワーク銀行 1341 の認証装置 1351 と、認証履歴を格納する認証履歴格納装置 14 とが、イン

ターネットなどのネットワーク（通信網）を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取引）の正当性を認証する。

本実施形態では、例えば、発注者 3 1 とネットワーク銀行 1 3 4 0 との間で認証を行うことに関する契約が成されており、受注者 3 3 とネットワーク銀行 1 3 4 1 との間で認証を行うことに関する契約が成されている。

また、ネットワーク銀行 1 3 4 0 とネットワーク銀行 1 3 4 1 とでは、認証に関して、相互に連携する旨の相互乗り入れの契約が成立されている。

本実施形態は、第 1 0 ～ 1 2 の発明に対応した実施形態である。

本実施形態では、発注者 3 1 が本発明の第 1 の取引者に対応し、受注者 3 3 が本発明の第 2 の取引者に対応している。

また、認証装置 1 3 5 0 が、第 1 1 の発明の認証装置、並びに第 1 0 の発明および第 1 2 の発明の第 1 の認証装置に対応している。

また、認証装置 1 3 5 1 が、第 1 1 の発明の他の認証装置、並びに第 1 0 の発明および第 1 2 の発明の第 2 の認証装置に対応している。

以下、トランザクション認証システム 1 3 0 1 を構成する各装置について説明する。

〔発注者端末装置 1 3 1 1 〕

図 1 8 に示すように、発注者端末装置 1 3 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 1 3 6 1、送信部 1 3 6 2、暗号化部 1 3 6 3、復号部 1 3 6 4、記憶部 1 3 6 5、制御部 1 3 6 6 および署名検証部 1 3 6 7 を有する。

なお、発注者端末装置 1 3 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 1 3 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な使用者であることを認証する生態認証部を有していてもよい。

受信部 1361 は、ネットワークを介して認証装置 1350 から情報あるいは要求を受信する。

送信部 1362 は、ネットワークを介して認証装置 1350 に情報あるいは要求を送信する。

また、受信部 1361 および送信部 1362 は、受注者 33 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 1363 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 1364 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 1365 は、例えば、発注者 31 がネットワーク銀行 1340 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵 $K_{31,s}$ などを格納する。

制御部 1366 は、発注者端末装置 1311 内の各構成要素の処理を統括的に制御する。

署名検証部 1367 は、例えば、認証装置 1350 が作成した署名情報を、ネットワーク銀行 1340 の公開鍵 $K_{40,p}$ を用いて検証する。

〔受注者端末装置 1315〕

図 19 に示すように、受注者端末装置 1315 は、サイバーモール (Cyber Mall) などに店舗を出している受注者 33 が使用するサーバ装置であり、受信部 1371、送信部 1372、暗号化部 1373、復号部 1374、記憶部 1375、制御部 1376 および署名検証部 1377 を有する。

受信部 1371 は、ネットワークを介して認証装置 1351 から情報あるいは要求を受信する。

送信部 1372 は、ネットワークを介して認証装置 1351 に情報あるいは要求を送信する。

また、受信部 1371 および送信部 1372 は、発注者端末装置 1311 から

のアクセスに応じて、例えば、記憶部 1 3 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 1 3 1 1 に送信する。

暗号化部 1 3 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 1 3 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 1 3 7 5 は、例えば、受注者 3 3 がネットワーク銀行 1 3 4 1 と契約を行うと、例えば、受注者 3 3 に割り当てられた秘密鍵 $K_{33, s}$ などを格納する。

制御部 1 3 7 6 は、受注者端末装置 1 3 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 1 3 7 7 は、例えば、受注者 3 3 の公開鍵 $K_{33, p}$ を用いて、受注者端末装置 1 3 1 5 が作成した署名情報の検証を行う。

〔認証装置 1 3 5 0〕

図 2 0 に示すように、認証装置 1 3 5 0 は、受信部 1 3 8 1、送信部 1 3 8 2、暗号化部 1 3 8 3、復号部 1 3 8 4、記憶部 1 3 8 5、制御部 1 3 8 6、署名作成部 1 3 8 7 および課金処理部 1 3 8 8 を有する。

ここで、受信部 1 3 8 1 および送信部 1 3 8 2 が、第 1 1 の発明の送受信手段に対応し、記憶部 1 3 8 5 が第 1 1 の発明の記憶手段に対応し、署名作成部 1 3 8 7 が第 1 1 の発明の署名作成手段に対応している。

受信部 1 3 8 1 は、ネットワークを介して発注者端末装置 1 3 1 1 および認証装置 1 3 5 1 から情報あるいは要求を受信する。

送信部 1 3 8 2 は、ネットワークを介して発注者端末装置 1 3 1 1 および認証装置 1 3 5 1 に情報あるいは要求を送信する。

暗号化部 1 3 8 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 1 3 8 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 1385 は、例えば、発注者 31 がネットワーク銀行 1340 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵 $K_{31, s}$ に対応する公開鍵 $K_{33, P}$ などを格納する。また、記憶部 1385 は、認証装置 1351 から受信した受注者 33 の銀行口座と振込連絡先を記憶する。

制御部 1386 は、認証装置 1350 内の各構成要素の処理を統括的に制御する。

署名作成部 1387 は、ネットワーク銀行 1340 の秘密鍵 $K_{40, s}$ を用いて署名情報の作成を行う。

課金処理部 1388 は、発注者 31 による取引に関する認証に対しての課金処理を行い、認証装置 1351 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

また、課金処理部 1388 は、発注者 31 から受けた支払いのうち、一部を受注者 33 に支払い、残りを手数料としてネットワーク銀行 1340 が受け取るための処理を行う。

認証装置 1350 の各構成要素の詳細な処理については、後述する動作例で記載する。

〔認証装置 1351〕

図 21 に示すように、認証装置 1351 は、受信部 1391、送信部 1392、暗号化部 1393、復号部 1394、記憶部 1395、制御部 1396、署名作成部 1397 および課金処理部 1398 を有する。

受信部 1391 は、ネットワークを介して受注者端末装置 1315 および認証装置 1350 から情報あるいは要求を受信する。

送信部 1392 は、ネットワークを介して受注者端末装置 1315 および認証装置 1350 に情報あるいは要求を送信する。

暗号化部 1393 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 1394 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 1395 は、受注者 33 がネットワーク銀行 1341 と契約を行うと、例えば、受注者 33 に割り当てられた秘密鍵 $K_{33, s}$ に対応する公開鍵 $K_{33, p}$ などを格納する。

制御部 1396 は、認証装置 1351 内の各構成要素の処理を統括的に制御する。

署名作成部 1397 は、ネットワーク銀行 1341 の秘密鍵 $K_{41, s}$ を用いて署名情報の作成を行う。

課金処理部 1398 は、受注者 33 による取引に関する認証に対しての課金処理を行い、認証装置 1350 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

以下、トランザクション認証システム 1301 の動作例を説明する。

以下に示す動作例を開始する前提として、発注者 31 とネットワーク銀行 1340 との間で所定の契約が結ばれ、ネットワーク銀行 1340 は、発注者 31 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行する。ネットワーク銀行 1340 は、個人キー情報 k_1 および個人 ID 情報 ID_1 の対応表を図 20 に示す認証装置 1350 の記憶部 1385 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 1340 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行 1340 は、自らの秘密鍵 $K_{40, s}$ を図 20 に示す認証装置 1350 の記憶部 1385 に記憶すると共に、当該秘密鍵 $K_{40, s}$ に対応する公開鍵 $K_{40, p}$ を発注者端末装置 1311 に送信する。発注者端末装置 1311 は、公開鍵 $K_{40, p}$ を図 18 に示す記憶部 1365 に記憶する。

また、受注者 33 とネットワーク銀行 1341 との間で所定の契約が結ばれ、ネットワーク銀行 1341 は、受注者 33 に対して、個人キー情報 Z および個人

I D 情報 I D 2 を発行する。ネットワーク銀行 1 3 4 1 は、個人キー情報 Z および個人 I D 情報 I D 2 の対応表を図 2 1 に示す認証装置 1 3 5 1 の記憶部 1 3 9 5 に記憶する。

また、ネットワーク銀行 1 3 4 1 は、自らの秘密鍵 $K_{41,s}$ を図 2 1 に示す認証装置 1 3 5 1 の記憶部 1 3 9 5 に記憶すると共に、当該秘密鍵 $K_{41,s}$ に対応する公開鍵 $K_{41,p}$ を受注者端末装置 1 3 1 5 に送信する。受注者端末装置 1 3 1 5 は、公開鍵 $K_{41,p}$ を図 1 9 に示す記憶部 1 3 7 5 に記憶する。

また、ネットワーク銀行 1 3 4 0 とネットワーク銀行 1 3 4 1 との間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置 1 3 5 0 と認証装置 1 3 5 1 との間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

図 2 2 A ~ 2 2 F および図 2 3 A ~ 2 3 F は、トランザクション認証システム 1 3 0 1 の動作例を説明するための図である。

ステップ S T 1 3 1 :

図 1 7 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、受注者 3 3 を特定する情報（例えば受注者 3 3 の名前）、発注する商品名および数量などを示す発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 とを、図示しない操作手段を操作して発注者端末装置 1 3 1 1 に入力する。なお、発注情報 a 1 には、受注者 3 3 を特定する情報、例えば受注者 3 3 の名前（商店名）が含まれている。

次に、図 1 8 に示す発注者端末装置 1 3 1 1 の暗号化部 1 3 6 3 は、記憶部 1 3 6 5 から読み出した所定の暗号鍵を用いて、発注情報 a 1 および個人キー情報 k 1 を暗号化し、当該暗号化した情報を格納した認証要求 I n f 1 （本発明の第 1 の要求）を、送信部 1 3 6 2 からネットワークを介して、図 1 7 に示すネットワーク銀行 1 3 4 0 の認証装置 1 3 5 0 に送信する。

ステップ S T 1 3 2 :

図 20 に示す認証装置 1350 は、発注者端末装置 1311 からの認証要求 I n f 1 を受信部 1381 が受信すると、記憶部 1385 から所定の暗号化鍵を読み出し、復号部 1384 において、当該暗号鍵を用いて認証要求 I n f 1 を復号する。

次に、認証装置 1350 は、制御部 1386 からの制御に基づいて、上記復号した認証要求 I n f 1 に格納された受注者 33 を特定する情報を含む要求 I n f 2 を生成し、これを送信部 1382 からネットワークを介して認証装置 1351 に送信する。

ステップ S T 133 :

認証装置 1351 は、認証装置 1350 から受信した要求 I n f 2 に応じて、当該要求 I n f 2 に含まれる情報によって特定された受注者 33 とネットワーク銀行 1341 との間に契約が結ばれているか否かを判断し、その判断結果を含む応答 I n f 3 (本発明の回答) を送信部 1392 からネットワークを介して認証装置 1350 に送信する。

ステップ S T 134 :

認証装置 1350 は、認証装置 1351 から受信した応答 I n f 3 が、受注者 33 の正当性を示している場合に以下の処理を行う。

認証装置 1350 は、ステップ S T 131 で受信した要求 I n f 1 に含まれる情報から個人キー k 1 を削除した情報 I n f 1' と、当該取り引きを識別するために生成されたトランザクション T r I D と、ネットワーク銀行 1340 の秘密鍵 $K_{40,s}$ を用いて生成した署名情報 A u - A 1 とを格納した要求 I n f 4 (本発明の第 2 の要求) を生成し、これをネットワーク銀行 1341 の公開鍵 $K_{41,p}$ で暗号化して送信部 1382 からネットワークを介して認証装置 1351 に送信する。

ステップ S T 135 :

認証装置 1351 は、認証装置 1350 から受信した要求 I n f 4 をネットワ

ーク銀行 1 3 4 1 の秘密鍵 $K_{41,s}$ を用いて復号し、これにネットワーク銀行 1 3 4 1 の秘密鍵 $K_{41,s}$ を用いて生成した署名情報 $Au-B1$ を付加して要求 $Inf5$ (本発明の第 3 の要求) を生成する。そして、要求 $Inf5$ を受注者 3 3 の公開鍵 $K_{33,p}$ を用いて暗号化した後に送信部 1 3 9 2 からネットワークを介して受注者端末装置 1 3 5 1 に送信する。

ステップ ST 1 3 6 :

受注者端末装置 1 3 5 1 は、認証装置 1 3 5 1 から受信した要求 $Inf5$ を受注者 3 3 の秘密鍵 $K_{33,s}$ を用いて復号して受注を確認すると、これに受注者 3 3 の秘密鍵 $K_{33,s}$ を用いて作成した署名情報 $Au-S$ を付加して応答 $Inf6$ (本発明の第 1 の応答) を生成する。そして、応答 $Inf6$ をネットワーク銀行 1 3 4 1 の公開鍵 $K_{41,p}$ を用いて暗号化した後に、送信部 1 3 7 2 からネットワークを介して認証装置 1 3 5 1 に送信する。

ステップ ST 1 3 7 :

認証装置 1 3 5 1 は、受注者端末装置 1 3 5 1 から受信した応答 $Inf6$ をネットワーク銀行 1 3 4 1 の秘密鍵 $K_{41,s}$ を用いて復号した後に、受注者 3 3 の銀行口座と振込連絡先を示す情報 f と、ネットワーク銀行 1 3 4 1 の秘密鍵 $K_{41,s}$ を用いて生成した署名情報 $Au-B2$ とを付加して応答 $Inf7$ (本発明の第 2 の応答) を生成する。そして、これをネットワーク銀行 1 3 4 1 の公開鍵 $K_{41,p}$ を用いて暗号化して送信部 1 3 9 2 からネットワークを介して認証装置 1 3 5 0 に送信する。

ステップ ST 1 3 8 :

認証装置 1 3 5 0 は、認証装置 1 3 5 1 から受信した応答 $Inf8$ をネットワーク銀行 1 3 4 0 の秘密鍵 $K_{40,s}$ を用いて復号した後に、応答 $Inf8$ から受注者 3 3 の銀行口座と振込連絡先を取り出し、これを記憶部 (データベース) 1 3 8 5 に格納する。

ステップ ST 1 3 9 :

認証装置 1350 は、応答 Inf 8 に含まれる Inf 7 から受注者 33 の銀行口座と振込連絡先を削除した情報と、ネットワーク銀行 1340 の秘密鍵 $K_{40,s}$ を用いて生成した署名情報 Au-A2 とを含む応答 Inf 8 を生成する。そして、これを発注者 31 の公開鍵 $K_{31,p}$ を用いて暗号化して送信部 1382 からネットワークを介して発注者端末装置 1311 に送信する。

ステップ ST 140 :

ネットワーク銀行 1340 の課金処理部 1388 は、予め登録した発注者 31 の銀行口座から、当該取引についての受注者 33 に支払う金額と手数料とを加算した金額を引き落とし、ネットワーク銀行 1340 の口座に振り込む。

ステップ ST 141 :

ネットワーク銀行 1340 の課金処理部 1388 は、ステップ ST 140 で引き落とした金額のうち受注者 33 に支払う金額を、ステップ ST 138 で得た受注者 33 の銀行口座に振り込むと共に、その旨を受注者 33 に通知する。

ステップ ST 142 :

ネットワーク銀行 1340 の課金処理部 1388 は、ステップ ST 140 で引き落とした金額のうち契約に基づく手数料の一部を、ネットワーク銀行 1341 の口座に振り込む。

以上説明したように、トランザクション認証システム 1301 によれば、認証装置 1350 から認証装置 1351 へは、発注者 31 の個人キー情報 k_1 を送信しないことから、発注者 31 の個人情報が、発注者 31 が契約していない他のネットワーク銀行 1341 に漏れることを回避できる。

また、トランザクション認証システム 1301 によれば、受注者 33 は、自らの契約した認証装置 1350 の署名情報 Au-B1 を検証することで、当該取引の正当性を確認できる。

上述したように、トランザクション認証システム 1301 によれば、異なる認証機関と契約をしている複数の取引引き者の間の取引引きに関する認証を、高い

信頼性で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取引引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行 1340, 1341 が、それぞれ認証装置 1350, 1351 を用いて、トランザクション（取引引き）の認証業務を行う場合を例示したが、ネットワーク銀行 1340, 1341 とは別の機関が、認証装置 1350, 1351 を用いてトランザクションの認証業務を行うようにしてもよい。

また、上述した実施形態では、発注者 31 が契約したネットワーク銀行 1340 の認証装置 1350 と、受注者 33 が契約したネットワーク銀行 1341 の認証装置 1351 との間で連携して認証処理を行う場合を例示したが、3 人以上の取引引き者がそれぞれ異なる認証機関と契約を行っている場合に、3 以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

第 5 実施形態

図 24 は、本実施形態の認証システム 801 の全体構成図である。

図 24 に示すように、認証システム 801 では、例えば、ユーザ 831 が使用する端末装置 811 と、ネットワーク銀行 821 が使用する認証装置 813 とが、インターネットなどのネットワーク（通信網）を介して接続されており、認証装置 813 がユーザ 831 の認証情報を提供する。

なお、当該ネットワークに接続されている端末装置 811 の数は任意である。

また、本実施形態では、ネットワーク銀行 821 が、認証装置 813 を使用する場合を例示するが、認証装置 813 はネットワーク銀行 821 以外の認証機関

本実施形態は、第 13 ～ 第 15 の発明に対応した実施形態であり、端末装置 811 が本発明の端末装置に対応し、認証装置 813 が本発明の認証装置に対応している。

以下、認証システム 8 0 1 を構成する各装置について説明する。

〔端末装置 8 1 1〕

図 2 5 は、端末装置 8 1 1 の機能ブロック図である。

図 2 5 に示すように、端末装置 8 1 1 は、例えば、ユーザ 8 3 1 が使用するパーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 8 6 1、送信部 8 6 2、暗号化部 8 6 3、復号部 8 6 4、記憶部 8 6 5、操作部 8 6 6、表示部 8 6 7、制御部 8 6 8 およびスマートカードアクセス部 8 6 9 を有する。

受信部 8 6 1 は、ネットワークを介して認証装置 8 1 3 から情報および要求を受信する。

送信部 8 6 2 は、ネットワークを介して認証装置 8 1 3 に情報および要求を送信する。

また、受信部 8 6 1 および送信部 8 6 2 は、ネットワークを介して、その他のサーバ装置あるいは端末装置との間で情報および要求を送受信する。

暗号化部 8 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 8 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 8 6 5 は、認証装置 8 1 3 から受信した認証情報 S I G b などを記憶する。ここで、認証情報 S I G b は、認証装置 8 1 3 が生成したユーザ 8 3 1 の認証情報 S I G を分割して得られた情報である。

操作部 8 6 6 は、キーボードやマウスなどであり、ユーザの操作に応じた操作信号を制御部 8 6 8 やスマートカードアクセス部 8 6 9 に出力する。

表示部 8 6 7 は、制御部 8 6 8 からの表示信号に応じた画像を表示する。

制御部 8 6 8 は、端末装置 8 1 1 内の各構成要素の処理を統括的に制御する。

制御部 8 6 8 の処理については、後述する動作例で詳細に説明する。

スマートカードアクセス部 8 6 9 は、例えばユーザによって端末装置 8 1 1 に

装着されたスマートカード 850 の IC メモリにアクセスを行う。

〔認証装置 813〕

図 26 は、認証装置 813 の機能ブロック図である。

図 26 に示すように、認証装置 813 は、例えば、受信部 881、送信部 882、暗号化部 883、復号部 884、記憶部 885、操作部 886、表示部 887、制御部 888 およびスマートカードアクセス部 889 を有する。

ここで、受信部 881 が本発明の受信手段に対応し、送信部 882 が本発明の送信手段に対応し、記憶部 885 が本発明の記憶手段に対応し、制御部 888 が本発明の制御手段に対応し、スマートカードアクセス部 889 が本発明の書込手段に対応している。

受信部 881 は、ネットワークを介して端末装置 811 から情報あるいは要求を受信する。

送信部 882 は、ネットワークを介して端末装置 811 に情報あるいは要求を送信する。

暗号化部 883 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 884 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 885 は、登録（契約）したユーザの個人情報、個人 ID 情報、後述するようにして生成された認証情報 SIG, SIGa, SIGb、並びに認証情報 SIGa のダウンロード先の装置 ID 情報などを記憶する。

ここで、認証情報 SIG が本発明の認証情報に対応し、認証情報 SIGa が本発明の第 1 の認証情報に対応し、認証情報 SIGb が本発明の第 2 の認証情報に対応している。

操作部 886 は、キーボードおよびマウスなどであり、ユーザの操作に応じた操作信号を制御部 888 に出力する。

表示部 887 は、制御部 888 からの表示信号に応じた画像を表示する。

制御部 888 は、認証装置 813 内の各構成要素の処理を統括的に制御する。

制御部 888 の処理については、後述する動作例で詳細に説明する。

スマートカードアクセス部 889 は、登録したユーザに発行するスマートカード 850 の IC メモリに、当該ユーザに対応する認証情報 SIG b を書き込む。

以下、認証システム 801 の動作例を説明する。

〔第 1 の動作例〕

ここでは、ネットワーク銀行 821 が認証情報 SIG を分割して得られた認証情報 SIG b を記憶されたスマートカード 850 を作成し、これをユーザ 831 に送付するまでの動作例を説明する。

図 27 は、当該動作例を説明するためのフローチャートである。

ステップ ST121 :

ユーザ 831 が図 25 に示す端末装置 811 の操作部 866 を操作して、登録要求と共に、自らの個人情報、並びに認証情報 SIG a のダウンロード先（送信先）として指定する単数または複数の端末装置（本実施形態では、端末装置 811）の装置 ID 情報を入力する。これにより、当該入力された情報を含む登録要求が、ネットワークを介して端末装置 811 の送信部 862 から認証装置 813 に送信される。

ステップ ST122 :

認証装置 813 は、ステップ ST1 で端末装置 811 から受信部 881 が受信した登録要求に応じて、ユーザ 831 に固有の個人 ID 情報を発行し、当該個人 ID 情報と、登録要求に含まれる個人情報およびダウンロード先の情報とを図 26 に示す記憶部 885 に書き込む。

ステップ ST123 :

認証装置 813 は、登録要求に応じて、公開鍵暗号化方式（PKI: Public Key Infrastructure）を用いて、ユーザ 831 の認証情報 SIG を生成する。

当該認証情報 S I G は、ユーザ 8 3 1 の個人認証に用いられる情報である。

ステップ S T 1 2 4 :

認証装置 8 1 3 は、ステップ S T 3 で生成した認証情報 S I G を、認証情報 S I G a と認証情報 S I G b とに分割する。

ステップ S T 1 2 5 :

認証装置 8 1 3 は、端末装置 8 1 1 の個人 I D 情報と関連付けて、認証情報 S I G, S I G a, S I G b を記憶部 8 8 5 に書き込む。

ステップ S T 1 2 6 :

認証装置 8 1 3 のスマートカードアクセス部 8 8 9 は、ユーザ 8 3 1 に発行するスマートカード 8 5 0 の I C メモリに、ユーザ 8 3 1 の個人 I D 情報および認証情報 S I G b を書き込む。

このとき、認証情報 S I G b は、図 2 6 に示す暗号化部 8 8 3 で暗号化された後に、スマートカード 8 5 0 の I C メモリに書き込まれてもよい。

ステップ S T 1 2 7 :

ネットワーク銀行 8 2 1 の担当者は、ステップ S T 6 の処理を経たスマートカード 8 5 0 を郵便などのオフラインでユーザ 8 3 1 に送付する。

ユーザ 8 3 1 は、ネットワーク銀行 8 2 1 が送付したスマートカード 8 5 0 を受け取る。

〔第 2 の動作例〕

当該動作例では、ユーザ 8 3 1 がスマートカード 8 5 0 を用いて、端末装置 8 1 1 で認証情報を得るときの動作例を説明する。

図 2 8 および図 2 9 は、当該動作例を説明するためのフローチャートである。

ステップ S T 1 3 1 :

ユーザ 8 3 1 は、スマートカード 8 5 0 を端末装置 8 1 1 のスマートカードアクセス部 8 6 9 に装着する。

ステップ S T 1 3 2 :

ユーザ 8 3 1 は、図 2 5 に示す操作部 8 6 6 を操作して、認証情報要求と共に、自らの個人 I D 情報と、ダウンロード先としての端末装置 8 1 1 の装置 I D 情報とを入力する。

これにより、当該入力された情報を含む認証情報要求がネットワークを介して端末装置 8 1 1 の送信部 8 6 2 から認証装置 8 1 3 に送信される。

ステップ S T 1 3 3 :

認証装置 8 1 3 の受信部 8 8 1 は、ステップ S T 1 2 で端末装置 8 1 1 が送信した認証情報要求を受信する。

ステップ S T 1 3 4 :

認証装置 8 1 3 の制御部 8 8 8 は、ステップ S T 1 3 で受信部 8 8 1 が受信した認証情報要求に含まれる個人 I D 情報に対応するダウンロード先の情報を図 2 6 に示す記憶部 8 8 5 から読み出し、当該読み出したダウンロード先の情報内に、認証情報要求に含まれるダウンロード先の情報に存在するか否かを判断し、存在すると判断した場合には認証情報要求が正当であるとし、存在しないと判断した場合には認証情報要求が不当であると判断する。

ステップ S T 1 3 5 :

認証装置 8 1 3 の制御部 8 8 8 は、認証情報要求が正当であると判断すると、認証情報要求に含まれる個人 I D 情報に対応する認証情報 S I G a を記憶部 8 8 5 から読み出し、当該読み出した認証情報 S I G a を、指定された装置 I D 情報によって特定される端末装置（本実施形態では、端末装置 8 1 1）に送信部 8 8 2 を介して送信する。

ステップ S T 1 3 6 :

一方、認証装置 8 1 3 の制御部 8 8 8 は、認証情報要求が不正であると判断すると、認証情報要求に含まれる個人 I D 情報に対応するダウンロード先の装置 I D 情報を記憶部 8 8 5 から読み出し、当該読み出した装置 I D 情報によって特定

される装置に、送信部 8 8 2 を介して、スマートカード 8 5 0 が不正に用いられた旨を示す通知を送信する。

ステップ S T 1 3 7 :

端末装置 8 1 1 の受信部 8 6 1 は、認証装置 8 1 3 から認証情報 S I G a を受信する。

ステップ S T 1 3 8 :

端末装置 8 1 1 の制御部 8 6 8 は、ステップ S T 1 4 で受信部 8 6 1 が受信した認証情報 S I G a と、スマートカード 8 5 0 に記憶されている認証情報 S I G b とが対応しているか否かを判断する。

ステップ S T 1 3 9 :

端末装置 8 1 1 の制御部 8 6 8 は、ステップ S T 1 8 で対応していると判断すると、ステップ S T 1 7 で受信部 8 6 1 が受信した認証情報 S I G a を記憶部 8 6 5 に書き込む。

これにより、端末装置 8 1 1 の制御部 8 6 8 は、記憶部 8 6 5 に記憶された認証情報 S I G a および S I G b を用いて認証情報 S I G を復元する。

ステップ S T 1 4 0 :

端末装置 8 1 1 の制御部 8 6 8 は、ステップ S T 1 6 で対応していないと判断すると、その旨を示す通知を、ネットワークを介して、送信部 8 6 2 から認証装置 8 1 3 に送信する。

ステップ S T 1 4 1 :

認証装置 8 1 3 の受信部 8 8 1 は、端末装置 8 1 1 から通知を受信する。

ステップ S T 1 4 2 :

認証装置 8 1 3 は、対応する正規に登録されたユーザの端末装置にスマートカード 8 5 0 が不正使用された旨を示す通知を送信部 8 8 2 から、ネットワークを介して送信する。

以上説明したように、認証システム 8 0 1 によれば、スマートカード 8 5 0 に

は、認証情報SIGの一部の認証情報SIGbのみを記憶し、端末装置811からの認証情報要求に応じて、認証装置813において、ユーザの正当性を検証した後、残りの認証情報SIGaを認証装置813から端末装置811に送信し、端末装置811内で認証情報SIGを復元するため、スマートカード850を盗難されたり、紛失した場合でも、不正なユーザは、スマートカード850だけでは認証情報SIGを得ることができない。そのため、スマートカード850を用いた、なりすましなどの不正利用を防止できる。

本発明は上述した実施形態には限定されない。

上述した実施形態では、ダウンロード先として、認証情報要求を送信する端末装置811を指定した場合を例示したが、その他の端末装置を指定することもできる。これにより、家庭内などに複数の端末装置がある場合に、一の端末装置にスマートカード850を装着すれば、他の端末装置でも、スマートカード850のユーザの認証情報を得ることができる。

第6実施形態

図30は、本実施形態のトランザクション認証システム401の全体構成図である。

図30に示すように、トランザクション認証システム401では、例えば、発注者31の発注者端末装置411と、受注者33の受注者端末装置415と、ネットワーク銀行440の認証装置450と、認証履歴を格納する認証履歴格納装置14とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者31と受注者33との間のトランザクション（取引）の正当性を認証装置450で認証する。

なお、当該ネットワークに接続されている発注者端末装置411および受注者端末装置415の数は任意である。

本実施形態では、発注者31の個人ID情報および個人キー情報は、受注者33には送られない。

本実施形態では、認証装置 4 5 0 が第 1 6 の発明の通信装置、並びに第 1 7 および第 1 8 の発明の第 1 の通信装置に対応し、受注者端末装置 4 1 5 あるいは不正者端末装置 4 5 6 が第 1 7 および第 1 8 の発明の第 2 の通信装置に対応している。

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 4 4 0 との間で認証を行うことに関する契約が成されている。また、発注者 3 1 と引き落とし銀行 4 4 2 との間では、例えば、ネットワーク銀行 4 4 0 によって認証された取引に関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 4 4 0 と保険会社 4 4 3 との間では、ネットワーク銀行 4 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

以下、トランザクション認証システム 4 0 1 を構成する各装置について説明する。

〔発注者端末装置 4 1 1〕

図 3 1 に示すように、発注者端末装置 4 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 4 6 1、送信部 4 6 2、暗号化部 4 6 3、復号部 4 6 4、記憶部 4 6 5、制御部 4 6 6 および署名検証部 4 6 7 を有する。

なお、発注者端末装置 4 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 4 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な利用者であることを認証する生体認証部を有していてもよい。

ここで、受信部 4 6 1 が第 1 7 の発明の第 2 の受信手段に対応し、送信部 4 6 2 が第 1 7 の発明の第 2 の送信手段に対応している。

受信部 4 6 1 は、ネットワークを介して認証装置 4 5 0 から情報あるいは要求

を受信する。

送信部 4 6 2 は、ネットワークを介して認証装置 4 5 0 に情報あるいは要求を送信する。

また、受信部 4 6 1 および送信部 4 6 2 は、受注者 3 3 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 4 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 4 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 4 6 5 は、発注者 3 1 が作成した秘密鍵 $K_{31,s}$ などを格納する。

署名検証部 4 6 7 は、例えば、認証装置 4 5 0 が作成した署名情報を、ネットワーク銀行 4 4 0 の公開鍵 $K_{40,p}$ を用いて検証する。

制御部 4 6 6 は、発注者端末装置 4 1 1 内の各構成要素の処理を統括的に制御する。

制御部 4 6 6 は、例えば、発注者 3 1 による操作に応じて、発注情報 a_1 と、個人キー情報 k_1 （本発明の利用者を識別するための個人識別情報）と、個人 ID 情報 ID_1 （本発明の個人識別情報）との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf_1 を生成する。

ここで、個人キー情報 k_1 および個人 ID 情報 ID_1 は、発注者 3 1 がネットワーク銀行 4 4 0 に自らを登録したときに、当該発注者 3 1 に割り当てられた固有の識別子である。例えば、個人キー情報 k_1 は、ネットワーク銀行 4 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、制御部 4 6 6 は、例えば、認証要求 Inf_1 を認証装置 4 5 0 に送信し

た後に、認証装置 4 5 0 から認証応答 I n f 4 を受信したときに、認証応答 I n f 4 に含まれる認証結果を所定の表示装置や音声出力装置を介して出力する制御を行なう。

〔受注者端末装置 4 1 5〕

図 3 2 に示すように、受注者端末装置 4 1 5 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 4 7 1、送信部 4 7 2、暗号化部 4 7 3、復号部 4 7 4、記憶部 4 7 5、制御部 4 7 6 および署名検証部 4 7 7 を有する。

受信部 4 7 1 は、ネットワークを介して認証装置 4 5 0 から情報あるいは要求を受信する。

送信部 4 7 2 は、ネットワークを介して認証装置 4 5 0 に情報あるいは要求を送信する。

また、受信部 4 7 1 および送信部 4 7 2 は、発注者端末装置 4 1 1 からのアクセスに応じて、例えば、記憶部 4 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 4 1 1 に送信する。

暗号化部 4 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 4 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 4 7 5 は、受注者 3 3 が作成した秘密鍵 $K_{33, s}$ などを格納する。

制御部 4 7 6 は、受注者端末装置 4 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 4 7 7 は、例えば、ネットワーク銀行 4 4 0 の公開鍵 $K_{40, p}$ を用いて、認証装置 4 5 0 が作成した署名情報の検証を行う。

〔認証装置 4 5 0〕

図 3 3 に示すように、認証装置 4 5 0 は、受信部 4 8 1、送信部 4 8 2、暗号化部 4 8 3、復号部 4 8 4、記憶部 4 8 5、制御部 4 8 6、署名作成部 4 8 7 お

よび課金処理部 4 8 8 を有する。

ここで、受信部 4 8 1 が、第 1 6 の発明の受信手段、並びに第 1 7 の発明の第 1 の受信手段に対応している。送信部 4 8 2 が、第 1 6 の発明の送信手段、並びに第 1 7 の発明の第 1 の送信手段に対応している。記憶部 4 8 5 が、第 1 6 の発明および第 1 7 の発明の記憶手段に対応している。制御部 4 8 6 が、第 1 6 の発明および第 1 7 の発明の処理手段に対応している。

受信部 4 8 1 は、ネットワークを介して発注者端末装置 4 1 1 および受注者端末装置 4 1 5 から情報あるいは要求を受信する。

送信部 4 8 2 は、ネットワークを介して発注者端末装置 4 1 1 および受注者端末装置 4 1 5 に情報あるいは要求を送信する。

暗号化部 4 8 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 4 8 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 4 8 5 は、発注者 3 1 がネットワーク銀行 4 4 0 と契約したときに、発注者 3 1 の個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者 3 1 のネットワーク ID_N （本発明の送信先の情報）との対応表を図 3 3 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶する。

ここで、ネットワーク ID_N は、発注者 3 1 がネットワーク銀行 4 4 0 にオンラインで登録した、当該ネットワークのユーザである発注者 3 1 をネットワーク内で一意に識別するための識別子である。

また、記憶部 4 8 5 は、例えば、発注者 3 1 および受注者 3 3 がネットワーク銀行 4 4 0 と契約をしたときに、発注者 3 1 が作成した秘密鍵 $K_{31,s}$ に対応する公開鍵 $K_{31,p}$ 、並びに受注者 3 3 が作成した秘密鍵 $K_{33,s}$ に対応する公開鍵 $K_{33,p}$ などを格納する。

制御部 4 8 6 は、認証装置 4 5 0 内の各構成要素の処理を統括的に制御する。

署名作成部 4 8 7 は、ネットワーク銀行 4 4 0 の秘密鍵 $K_{40,s}$ を用いて署名情報の作成を行う。

課金処理部 4 8 8 は、発注者 3 1 による取り引きに関する認証に対しての課金処理を行う。

認証装置 4 5 0 の各構成要素の詳細な処理については、後述する動作例で記載する。

以下、トランザクション認証システム 4 0 1 の動作例を説明する。

当該動作例を開始する前提として、発注者 3 1 とネットワーク銀行 4 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 4 0 は、発注者 3 1 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行している。

また、発注者 3 1 は、ネットワーク内で当該発注者 3 1 を識別するネットワーク ID N を、秘密が保持される環境、例えばオフラインでネットワーク銀行 4 4 0 に登録している。

ネットワーク銀行 4 4 0 は、個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者 3 1 のネットワーク ID N との対応表を図 3 3 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶している。

また、ネットワーク銀行 4 4 0 は、自らの秘密鍵 $K_{40,s}$ を図 3 3 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶すると共に、当該秘密鍵 $K_{40,s}$ に対応する公開鍵 $K_{40,p}$ を発注者端末装置 4 1 1 および受注者端末装置 4 1 5 に送信する。発注者端末装置 4 1 1 は、公開鍵 $K_{40,p}$ を図 3 1 に示す記憶部 4 6 5 に記憶する。受注者端末装置 4 1 5 は、公開鍵 $K_{40,p}$ を図 3 2 に示す記憶部 4 7 5 に記憶する。

また、受注者 3 3 とネットワーク銀行 4 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 4 0 は、受注者 3 3 に対して、受注者を特定する情報 Z および個人 ID 情報 ID_2 を発行する。ネットワーク銀行 4 4 0 は、情報 Z および個人 ID 情報 ID_2 の対応表を図 3 3 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶する。

以下、発注者 3 1 が、認証装置 4 5 0 に認証要求を行なった場合のトランザクション認証システム 4 0 1 の動作を説明する。

図 3 4 A ~ 3 4 D は、トランザクション認証システム 4 0 1 の当該動作を説明するための図である。

ステップ S T 4 1 :

図 3 0 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 と、発注者 3 1 の個人 I D 情報 I D 1 とを、図示しない操作手段を操作して発注者端末装置 4 1 1 に入力する。なお、発注情報 a 1 には、受注者 3 3 を特定する情報が含まれている。

次に、図 3 1 に示す発注者端末装置 4 1 1 の暗号化部 4 6 3 は、記憶部 4 6 5 から読み出したネットワーク銀行 4 4 0 の公開鍵 $K_{40, P}$ を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 I D 情報 I D 1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 I n f 1 (本発明の要求) を、送信部 4 6 2 からネットワークを介して、図 3 0 に示すネットワーク銀行 4 4 0 の認証装置 4 5 0 に送信する。

ステップ S T 4 2 :

図 3 3 に示す認証装置 4 5 0 は、発注者端末装置 4 1 1 からの認証要求 I n f 1 を受信部 4 8 1 が受信すると、記憶部 4 8 5 からネットワーク銀行 4 4 0 の秘密鍵 $K_{40, S}$ を読み出し、復号部 4 8 4 において、当該秘密鍵 $K_{40, S}$ を用いて認証要求 I n f 1 を復号する。

次に、認証装置 4 5 0 は、制御部 4 8 6 の制御に基づいて、上記復号した認証要求 I n f 1 から個人キー情報 k 1 および個人 I D 情報 I D 1 を削除した情報 I n f 1' について、記憶部 4 8 5 から読み出した自らの秘密鍵 $K_{40, S}$ を用いて署名情報 A u 1 を作成する。

次に、認証装置 4 5 0 は、情報 I n f 1' および署名情報 A u 1 を格納した要

求 I n f 2 を生成する。

次に、暗号化部 4 8 3 は、図 3 3 に示す記憶部 4 8 5 から読み出した受注者 3 3 の公開鍵 $K_{33, P}$ を用いて、上記生成した要求 I n f 2 を暗号化した後に、送信部 4 8 2 から、ネットワークを介して受注者端末装置 4 1 5 に送信する。

ステップ S T 4 3 :

受注者端末装置 4 1 5 の復号部 4 7 4 は、認証装置 4 5 0 からの要求 I n f 2 を受信部 4 7 1 が受信すると、記憶部 4 7 5 から読み出した自らの秘密鍵 $K_{33, s}$ を用いて、要求 I n f 2 を復号する。

次に、受注者端末装置 4 1 5 の署名検証部 4 7 7 は、上記復号した要求 I n f 2 に格納された署名情報 A u 1 を、記憶部 4 7 5 から読み出した認証装置 4 5 0 の公開鍵 $K_{40, P}$ を用いて検証する。

受注者端末装置 4 1 5 の制御部 4 7 6 は、署名検証部が上記検証の結果、署名情報 A u 1 の正当性が認証されると、要求 I n f 2 に格納された情報 I n f 1' を図 3 2 に示す記憶部 4 7 5 に記憶する。受注者 3 3 は、情報 I n f 1' 内の発注情報 a 1 に基づいて、発注者 3 1 への商品等の発送予定などを示す受注確認情報 c 1 を生成する。

次に、制御部 4 7 6 は、要求 I n f 2、受注確認情報 c 1 および自らを特定する情報 Z を格納した応答 I n f 3 を生成する。

次に、受注者端末装置 4 1 5 の送信部 4 7 2 は、上記生成した応答 I n f 3 を、記憶部 4 7 5 から読み出したネットワーク銀行 4 4 0 の公開鍵 $K_{40, P}$ を用いて暗号化部 4 7 3 で暗号化した後に、送信部 4 7 2 から、ネットワークを介して認証装置 4 5 0 に送信する。

受注者 3 3 は、例えば、要求 I n f 2 に格納された情報 I n f 1' 内の発注情報 a 1 に基づいて、発注者 3 1 が発注した商品等を発注者 3 1 に発送したり、発注者 3 1 が注文したサービスを発注者 3 1 に提供する。

ステップ S T 4 4 :

認証装置 450 の復号部 484 は、受注者端末装置 415 からの応答 Inf 3 を受信部 481 が受信すると、記憶部 485 から読み出した自らの秘密鍵 $K_{40,s}$ を用いて、Inf 3 を復号し、要求 Inf 1 に格納された発注情報 a 1 と、当該復号された Inf 3 に格納された受注者 33 の情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 485 に格納する。当該履歴情報は、ネットワーク銀行 440 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 450 の署名作成部 487 は、ステップ ST 43 で受信した応答 Inf 3 について、自らの秘密鍵 $K_{40,s}$ を用いて署名情報 Au 2 を作成する。

次に、認証装置 450 の制御部 486 は、応答 Inf 3 および署名情報 Au 2 を格納した認証応答 Inf 4 を作成する。

次に、認証装置 450 の暗号化部 483 は、上記作成し認証した応答 Inf 4 を、公開鍵 $K_{31,p}$ を用いて暗号化した後に、個人 ID 情報 ID 1 に対応する記憶部 485 から読み出した発注者 31 のネットワーク ID_N に基づいて送信先を特定して、送信部 482 からネットワークを介して発注者端末装置 411 に送信する。

発注者端末装置 411 では、受信した認証応答 Inf 4 を、図 31 に示す記憶部 465 から読み出した発注者 31 の秘密鍵 $K_{31,s}$ を用いて復号部 464 で復号する。

次に、発注者端末装置 411 の署名検証部 466 は、当該復号した認証応答 Inf 4 に格納された署名情報 Au 2 を、記憶部 465 から読み出したネットワーク銀行 440 の公開鍵 $K_{40,p}$ を用いて検証する。

当該検証によってその正当性が確認されると、制御部 466 は、認証応答 Inf 4 に格納されている発注情報 a 1 や取り引きの内容を示す情報に応じた出力を、発注者端末装置 411 の図示しないディスプレイやスピーカから出力する。

以下、発注者 31 の個人 ID 1 および個人キー k 1 を不正に取得した図 30 に

示す不正者 5 5 が自らの端末装置である不正者端末装置 4 5 6 を用いて、認証装置 4 5 0 に認証要求を送信した場合のトランザクション認証システム 4 0 1 の動作を説明する。

ここで、不正者端末装置 4 5 6 の構成は、例えば、図 3 1 に示す発注者端末装置 4 1 1 と同じである。

図 3 5 A ~ 3 5 D は、トランザクション認証システム 4 0 1 の当該動作を説明するための図である。

ステップ S T 5 1 :

図 3 0 に示す不正者 5 5 は、受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、不正に取得した発注者 3 1 の個人キー情報 k 1 と、不正に取得した発注者 3 1 の個人 I D 情報 I D 1 とを、図示しない操作手段を操作して不正者端末装置 4 5 6 に入力する。

次に、不正者端末装置 4 5 6 の図 3 1 に示す暗号化部 4 6 3 は、記憶部 4 6 5 から読み出したネットワーク銀行 4 4 0 の公開鍵 $K_{40, P}$ を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 I D 情報 I D 1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 I n f 1 を、送信部 4 6 2 からネットワークを介して、図 2 3 A ~ 2 3 F に示すネットワーク銀行 4 4 0 の認証装置 4 5 0 に送信する。

ステップ S T 5 2 :

図 3 3 に示す認証装置 4 5 0 は、不正者端末装置 4 5 6 からの認証要求 I n f 1 を受信部 4 8 1 が受信すると、当該認証要求 I n f 1 について、前述したステップ S T 4 2 と同様の処理を行なう。

ステップ S T 5 3 :

ステップ S T 5 3 の処理は、前述したステップ S T 4 3 の処理と同じである。

ステップ S T 5 4 :

ステップ S T 5 4 の処理は、前述したステップ S T 4 4 の処理と同じである。

すなわち、不正者 5 5 が不正者端末装置 4 5 6 を用いて、認証要求 I n f 1 を認証装置 4 5 0 に送信した場合でも、その応答である認証応答 I n f 4 は、認証装置 4 5 0 の記憶部 4 8 5 に記憶されている発注者 3 1 のネットワーク I D _ N に基づいて、発注者端末装置 4 1 1 に送信される。

これにより、発注者 3 1 は、受信した認証応答 I n f 4 に基づいて、自らが個人 I D 情報 I D 1 を用いた不正な認証要求が行なわれたことを知ることができ、その旨をネットワーク銀行 4 4 0 などに通知する。

以上説明したように、トランザクション認証システム 4 0 1 によれば、認証装置 4 5 0 は、発注者 3 1 がネットワーク銀行 4 4 0 にオンラインで登録したネットワーク I D _ N によって指定された送信先に、認証応答 I n f 4 を送信するため、例えば、発注者 3 1 の個人情報 I D 1 を不正に取得した者が当該個人情報 I D 1 を用いて認証装置 4 5 0 に認証要求を行なった場合に、認証装置 4 5 0 に登録されたネットワーク I D _ N に基づいて認証装置 4 5 0 から発注者端末装置 4 1 1 に送信された認証応答 I n f 4 によって、発注者 3 1 は自らの個人情報 I D 1 を用いた不正な取り引きが行なわれることを知ることができる。

そのため、トランザクション認証システム 4 0 1 によれば、他人の個人 I D 情報を用いた不正な取り引きを効果的に抑制できる。

上述したように、トランザクション認証システム 4 0 1 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の処理手段が行う処理として認証処理を例示したが、その他、課金処理などの処理を行う場合にも本発明は適用可能である。

また、上述した実施形態では、ネットワーク銀行 440 が、認証装置 450 を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行 440 とは別の機関が、認証装置 450 を用いてトランザクションの認証業務を行うようにしてもよい。

第 7 実施形態

図 36 は、本実施形態におけるトランザクション認証システム 901 の構成を示した構成図である。

トランザクション認証システム 901 は、発注者 31 が発注処理を行う発注者端末装置 911 と、発注者 31 の生体的特徴を利用して発注者 31 が本人であることを認証する生体認証装置 12 と、ネットワーク銀行（あるいはトランザクション認証局運営会社） 921 によって使用され、商取引情報の認証を行う認証装置 913 と、認証履歴を格納する認証履歴格納装置 914 と、受注者 33 が受注処理を行う受注者端末装置 915 とを有する。

本実施形態では、発注者 31 の個人 ID 情報および個人キー情報は、受注者 33 には送られない。

本実施形態は、第 19～21 の発明に対応した実施形態であり、発注者端末装置 911 が本発明の第 1 の通信装置に対応し、認証装置 913 が本発明の認証装置に対応し、受注者端末装置 915 が本発明の第 2 の通信装置に対応している。また、発注者 31 が本発明の第 1 の取引引き者に対応し、受注者 33 が本発明の第 2 の取引引き者に対応している。

〔発注者端末装置 911〕

図 37 は、発注者端末装置 911 の機能ブロック図である。

発注者端末装置 911 は、本システム利用の契約を行った一般利用者である発注者 31 が使用する端末装置である。

発注者端末装置 911 は、図 37 に示すように、認証要求入力部 911a、認証要求送信部 911b、認証応答受信部 911c、認証要求暗号化部 911d お

よび認証応答復号部 9 1 1 e を有する。

認証要求入力部 9 1 1 a は、例えば、発注者 3 1 によるキーボードなどの操作に応じて、発注情報 a 1 および発注者個人キー情報 k 1（本発明の第 1 の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報 a 1 には、例えば、発注者 3 1 の名前、住所、連絡先、受注者 3 3 の個人キー情報 k 2（本発明の第 2 の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部 9 1 1 b は、認証要求入力部 9 1 1 a に入力された発注情報 a 1 および発注者個人キー情報を含む認証要求 I n f 1（本発明の第 1 の要求）を認証装置 9 1 3 に送信する。

認証応答受信部 9 1 1 c は、認証装置 9 1 3 から認証応答 I n f 4 を受信する。

認証要求暗号化部 9 1 1 d は、認証要求 I n f 1 を暗号化する。

認証応答復号部 9 1 1 e は、認証応答 I n f 4 を復号する。

〔生体認証装置 9 1 2〕

生体認証装置 9 1 2 は、いわゆるバイオメトリックス (biometrics) を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置 1 2 に格納しておいた利用者（発注者 3 1）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置 9 1 2 の記録装置は、外部から電氣的に切断されており、その情報が外部に流出しない構成となっている。

〔認証装置 9 1 3〕

図 3 8 は、認証装置 9 1 3 の機能ブロック図である。

認証装置 9 1 3 は、本システムを運営するネットワーク銀行 9 2 1 が使用する

装置である。

認証装置 9 1 3 は、図 3 8 に示すように、認証要求受信部 9 1 3 a、発注者認証部 9 1 3 b、要求生成部 9 1 3 c、要求送信部 9 1 3 d、応答受信部 9 1 3 e、受注者認証部 9 1 3 f、認証応答生成部 9 1 3 g、認証応答暗号化部 9 1 3 h、認証応答送信部 9 1 3 i、要求暗号化部 9 1 3 j、応答復号部 9 1 3 k、認証要求復号部 9 1 3 l、トランザクション ID 発行部 9 1 3 m および決済処理部 9 1 3 n を有する。

ここで、認証要求受信部 9 1 3 a が本発明の第 1 の受信手段に対応し、発注者認証部 9 1 3 b および要求生成部 9 1 3 c が本発明の第 1 の認証手段に対応し、要求送信部 9 1 3 d が本発明の第 1 の送信手段に対応し、応答受信部 9 1 3 e が本発明の第 2 の受信手段に対応し、受注者認証部 9 1 3 f および認証応答生成部 9 1 3 g が本発明の第 2 の認証手段に対応し、認証応答送信部 9 1 3 i が本発明の第 2 の送信手段に対応し、トランザクション ID 発行部 9 1 3 m が本発明の取り引き識別情報発行手段に対応し、決済処理部 9 1 3 n が本発明の決済処理手段に対応している。

認証要求受信部 9 1 3 a は、発注者端末装置 9 1 1 が送信した認証要求 I n f 1 を受信する。

発注者認証部 9 1 3 b は、認証要求 I n f 1 が含む発注者個人キー情報 k 1 を用いて発注者 3 1 の認証を行い、認証情報 A u 1（本発明の第 1 の認証情報）を生成する。

要求生成部 9 1 3 c は、認証要求 I n f 1 から個人キー情報 k 1 を削除して情報 I n f 1 a を生成し、当該情報 I n f 1 a と認証情報 A u 1 とを含む要求 I n f 2（本発明の第 2 の要求）を生成する。

要求送信部 9 1 3 d は、要求 I n f 2 を受注者端末装置 9 1 5 に送信する。

応答受信部 9 1 3 e は、受注者端末装置 9 1 5 から応答 I n f 3（本発明の応答）を受信する。

受注者認証部 913f は、応答 Inf 3 に含まれる受注者 33 の識別情報である個人キー情報 k 2、並びにトランザクション ID（本発明の取引引き識別情報）を用いて受注者 33 の認証を行い、認証情報 Au 2（本発明の第 2 の識別情報）を生成する。

認証応答生成部 913g は、応答 Inf 3 に認証情報 Au 2 を付加して認証応答 Inf 4 を生成する。

認証応答暗号化部 913h は、認証応答 Inf 4 を暗号化する。

認証応答送信部 913i は、暗号化された認証応答 Inf 4 を発注者端末装置 911 に送信する。

要求暗号化部 913j は、要求生成部 913c が生成した要求 Inf 2 を暗号化する。

応答復号部 913k は、応答 Inf 3 を復号する。

認証要求復号部 913l は、認証要求 Inf 1 を復号する。

トランザクション ID 発行部 913m は、認証要求受信部 913a が発注者端末装置 911 から認証要求 Inf 1 を受信したときに、当該認証要求 Inf 1 に係わる取引引きを識別するためのトランザクション ID を発行する。

決済処理部 913n は、発注者 31 と受注者 33 との間の取引引きの決済処理を、引き落とし銀行 142 のサーバ装置と通信しながら行う。

〔認証履歴格納装置 914〕

図 38 に示すように、認証履歴格納装置 914 は、認証履歴生成部 914a および認証履歴記憶部 914b を有する。

認証履歴生成部 914a は、発注者 31 から認証要求 Inf 1 を受信したことを示す履歴情報、受注者 33 に要求 Inf 2 を送信したことを示す履歴情報、受注者 33 から応答 Inf 3 を受信したことを示す履歴情報、発注者 31 に認証応答 Inf 4 を送信したことを示す履歴情報を生成し、これらを認証要求 Inf 1 の受信時にトランザクション ID 発行部 913m によって発行されたトランザク

ションIDに関連付けて、認証履歴記憶部914bに記憶する。

〔受注者端末装置915〕

図39は、受注者端末装置915の機能ブロック図である。

受注者端末装置915は、本システム利用の契約を行った商品販売業者等である商品の受注者33が使用する。

受注者端末装置915は、要求受信部915a、要求復号部915b、応答入力部915c、応答生成部915d、応答暗号化部915eおよび応答送信部915fを有する。

要求受信部915aは、認証装置913から要求Inf2を受信する。

要求復号部915bは、要求Inf2を復号する。

応答入力部915cは、ユーザによる操作に応じて、受注確認情報C1および受注者33を特定する情報Zを入力する。

応答生成部915dは、要求Inf2、受注確認情報C1および受注者33の情報Zを含む応答Inf3を生成する。

応答暗号化部915eは、応答Inf3を暗号化する。

応答送信部915fは、暗号化された応答Inf3を認証装置913に送信する。

本実施形態のトランザクション認証システム901では、電子商取引の当事者である発注者31と受注者33との間に、その商取引の第三者であるネットワーク銀行921（あるいはトランザクション認証局）が介在し、ネットワーク銀行921が当事者間で行われる電子商取引を認証装置913を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム901の利用を希望する商取引当事者は、まず、このネットワーク銀行921との間で認証装置13の利用契約を結ぶ。

例えば、図36に示すように、発注者31は、インターネット、郵便等を用い、ネットワーク銀行（トランザクション認証局運営会社）21に対して、契約に

必要な情報の送付を行う。ここで送付する情報としては、発注者 3 1 の氏名、住所等の他、代金等の落とし先となる発注者 3 1 が契約している引き落とし銀行 1 4 2 の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行 9 2 1 は、契約を行った発注者 3 1 に対し、銀行 1 4 2 からの代金引き落としの際にその正当性を証明する個人 I D 情報、および本システムにおいて発注者 3 1 を識別するための個人キー情報の発行を行う。ここで発行された個人 I D 情報は銀行 1 4 2 に対しても送られ、銀行 1 4 2 は、商品等の代金引き落としの際にこの個人 I D 情報を認証し、代金の不正引き落としを防止する。

なお、図 3 6 では、発注者 3 1 が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者 3 3 も同様な手順によりネットワーク銀行 9 2 1 との利用契約を結ぶ。また、ここでは、個人 I D 情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人 I D 情報としても利用できることとし、別個の個人 I D 情報を発行しない形態としてもよい。

次に、トランザクション認証システム 9 0 1 の動作について説明する。

図 4 0 および図 4 1 は、トランザクション認証システム 9 0 1 の動作を説明するためのフローチャートである。

ステップ S T 9 1 :

電子商取引によって商品を購入しようとする発注者 3 1 は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者 3 1 は、次に、発注者 3 1 が所有する図 3 7 に示す発注者端末装置 9 1 1 を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部 9 1 1 a を用い、購入を希望する商品・数量等を指定する発注情報 a 1 および発注者 3 1 の個人キー情報である発注者個人キー情報 k 1 を入力することにより行う。ここで、発注者個人キー情報 k 1 の入力、発注処理を行うたびに発注者 3 1 が手動で行うこととしてもよいし、発注処理時

、自動的に入力されることとしてもよい。

これにより、入力された発注情報 a 1 および発注者個人キー情報 k 1 を含む認証要求 I n f 1 が生成される。

このとき、認証要求送信部 9 1 1 b は、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求 I n f 1 の送信を禁止する不正送信防止機能を有しており、この状態ではステップ S T 9 2 の処理は行われない。

そのため、電子商取引を行おうとする発注者 3 1 は、生体認証装置 1 2 を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置 1 2 が発注者 3 1 の指紋によって発注者 3 1 を認証するものであった場合、発注者 3 1 は、生体認証装置 1 2 に自己の指紋を読み取らせ、発注者 3 1 の指紋を読み取った生体認証装置 1 2 は、読み取った指紋と、事前に取得し、内部に格納しておいた発注者 3 1 本人の指紋データとを照合し、読み取った指紋が発注者 3 1 本人のものであるか否か判断する。

そして、読み取った指紋が発注者 3 1 本人のものであると判断された場合、生体認証装置 1 2 は、認証が成立した旨の情報を認証要求送信部 9 1 1 b に指示を与え、この情報を受けた認証要求送信部 9 1 1 b は、不正送信防止機能を解除し、送られた認証要求をトランザクション認証局 3 2 所有の認証装置 9 1 3 に送信する。

ステップ S T 9 2 :

ステップ S T 9 1 で生成された認証要求 I n f 1 が認証要求暗号化部 9 1 1 d で暗号化された後、認証要求送信部 9 1 1 b を介して認証装置 9 1 3 に送信される。

図 3 8 に示す認証装置 9 1 3 に送信された認証要求 I n f 1 は、認証要求受信部 9 1 3 a で受信され、認証要求復号部 9 1 3 1 によって復号された後、発注者認証部 9 1 3 b に送られる。

次に、発注者認証部 9 1 3 b において、認証要求 I n f 1 に含まれる発注者個

人キー情報 k_1 と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者 31 であるか否かが判断される。

そして、正当な発注者 31 であると判断されると、ステップ ST93 の処理が行われる。

ステップ ST93 :

図 38 に示す認証装置 913 のトランザクション ID 発行部 913m において、ステップ ST92 で受信した認証要求 Inf1 に係わる取り引きを識別するトランザクション ID (IDTr) が発行される。

ステップ ST94 :

認証履歴格納装置 914 の認証履歴生成部 914a において、ステップ ST93 で生成されたトランザクション ID (IDTr) に、ステップ ST92 で発注者端末装置 911 から認証要求 Inf1 を受信したことを示すステータスコード STC1 が付加される。

そして、ステータスコード STC1 が付加された認証要求 Inf1 が認証履歴記憶部 914b に書き込まれる。

ステップ ST95 :

ステップ ST93 で受信した認証要求 Inf1 が要求生成部 913c に送られて、要求生成部 913c において、認証要求 Inf1 から個人キー情報 k_1 を削除して生成された情報 Inf1a と、認証情報 Au1 と、トランザクション ID (IDTr) を含む要求 Inf2 (本発明の第 2 の要求) が生成される。

ステップ ST96 :

ステップ ST95 で生成された要求 Inf2 が、要求暗号化部 913j において暗号化された後に、要求送信部 913d を介して受注者端末装置 915 に送信される。

受注者端末装置 915 に送信された要求 Inf2 は、要求受信部 915a によって受信された後、要求復号部 915b により復号される。

ステップ S T 9 7 :

認証履歴格納装置 9 1 4 の認証履歴生成部 9 1 4 a によって、ステップ S T 4 で認証履歴記憶部 9 1 4 b に書き込まれたトランザクション I D (I D T r) に、ステップ S T 9 6 で要求 I n f 2 を受注者端末装置 9 1 5 に送信したことを示すステータスコード S T C 2 が付加される。

このとき、当該トランザクション I D (I D T r) に、ステータスコード S T C 1 が既に付加されているかを確認し、付加されていない場合には、エラー処理を行う。

ステップ S T 9 8 :

受注者 3 3 は、ステップ S T 6 で復号された要求 I n f 2 に基づいて商品の受注処理を行う。

受注処理は、受注者 3 3 が応答入力部 9 1 5 c を用い、受注確認情報 C 1 および受注者 3 3 を特定する情報 Z を入力することにより行われる。ここで、情報 Z の入力、受注処理を行うたびに受注者 3 3 が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

ステップ S T 9 9

受注者端末装置 9 1 5 の応答生成部 9 1 5 d において、要求 I n f 2、受注確認情報 C 1 および受注者 3 3 の情報 Z を含む応答 I n f 3 が生成される。

ステップ S T 1 0 0 :

ステップ S T 9 9 で生成された応答 I n f 3 が、受注者端末装置 9 1 5 の応答暗号化部 9 1 5 e で暗号化された後に、応答送信部 9 1 5 f を介して認証装置 9 1 3 に送信される。

認証装置 9 1 3 に送信された応答 I n f 3 は、図 3 8 に示す応答受信部 9 1 3 e で受信され、応答復号部 9 1 3 k によって復号される。

ステップ S T 1 0 1 :

認証履歴格納装置 9 1 4 の認証履歴生成部 9 1 4 a によって、ステップ S T 4

で認証履歴記憶部 9 1 4 b に書き込まれたトランザクション ID に、ステップ S T 1 0 0 で応答 I n f 3 を受注者端末装置 9 1 5 から受信したことを示すステータスコード S T C 3 が付加される。

このとき、当該トランザクション ID (I D T r) に、ステータスコード S T C 1 , S T C 2 が既に付加されているかを確認し、付加されていない場合には、エラー処理を行う。

ステップ S T 1 0 2 :

ステップ S T 1 0 0 で受信した応答 I n f 3 が受注者認証部 9 1 3 f に送られる。

そして、受注者認証部 9 1 3 f において、応答 I n f 3 に含まれる情報 Z と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者 3 3 であるか否かが判断される。

そして、正当な受注者 3 3 であると判断されると、応答 I n f 3 は認証応答生成部 9 1 3 g に送られて、認証応答生成部 9 1 3 g において、応答 I n f 3 と、認証が成立したことを示す認証情報 A u 2 とを含む認証応答 I n f 4 が生成される。

ステップ S T 1 0 3 :

ステップ S T 1 0 2 で生成された認証応答 I n f 4 は、認証応答暗号化部 9 1 3 h において暗号化された後に、認証応答送信部 9 1 3 i を介して発注者端末装置 9 1 1 に送信される。

発注者端末装置 9 1 1 に送信された認証応答 I n f 4 は、図 3 7 に示す認証応答受信部 9 1 1 c で受信された後、認証応答復号手投 1 1 e によって復号され、発注者 3 1 は、この復号された認証応答 I n f 4 を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。

ステップ S T 1 0 4 :

認証履歴格納装置 9 1 4 の認証履歴生成部 9 1 4 a によって、ステップ S T 9

4で認証履歴記憶部914bに書き込まれたトランザクションID (IDTr) に、ステップST103で認証応答Inf4を発注者端末装置911に送信したことを示すステータスコードSTC4が付加される。

ステップST105：

決済処理部913nからの指示に応じて、ネットワーク銀行21は、発注者31の個人キー情報k1を用いて、発注者31が契約する引き落とし銀行142の銀行口座から、当該取り引きに伴う金額を引き落とす。当該引き落としは、ネットワーク銀行21の銀行口座に引き落とししてから受注者33の銀行口座に振り込んでもよいし、発注者31の銀行口座から受注者33の銀行口座に振り込みを直接行ってもよい。

また、受注者33は、発注情報a1に基づいて、発注者31に商品およびサービスを提供する。

ステップST106：

認証履歴生成部914aによって、決済処理が終了したことを示すステータスコードSTC5が生成され、ステータスコードSTC5が当該トランザクションID (Tr) に付加される。

以上説明したように、トランザクション認証システム901によれば、認証装置913において、発注者31および受注者33との間で行われた一連の手続きの履歴情報を管理するため、受注者33が故意にあるいは過失により、トランザクションIDを用いて、一つの受注に対して、引き落とし銀行142の発注者31の口座から複数回の引き落としが行われることを効果的に回避できる。

また、トランザクション認証システム901によれば、トランザクションIDを不正に用いたなりすまし行為を容易に発見でき対処できる。

また、トランザクション認証システム901によれば、発注者端末装置911および受注者端末装置915を用いた、発注者31と受注者33との間の電子商取引を認証装置913を用いて認証することで、電子商取引の信頼性を高めるこ

とができる。

また、トランザクション認証システム 9 0 1 によれば、認証装置 9 1 3 から受注者端末装置 9 1 5 に送信される要求 I n f 2 には、受注者 3 3 の個人キー情報 k 1 を含まないため、発注者 3 1 の課金に係わる個人キー情報が受注者 3 3 に渡ることではない。そのため、個人キー情報の不正利用を効果的に抑制できる。

また、トランザクション認証システム 9 0 1 によれば、第三者が発注者個人キー情報 k 1 を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答 I n f 4 は正規の発注者 3 1 に送信されることとなり、正規の発注者 3 1 は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

また、認証装置 9 1 3 によって、認証要求 I n f 1 および応答 I n f 3 を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

さらに、認証履歴格納装置 9 1 4 によって、認証要求 I n f 1 および応答 I n f 3 を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

また、認証要求 I n f 1、要求 I n f 2、応答 I n f 3 および認証応答 I n f 4 は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

さらに、認証要求送信部 9 1 1 b は、生体認証装置 1 2 によって発注者 3 1 が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

第 8 実施形態

図４２は、本実施形態のトランザクション認証システム５０１の全体構成図である。

図４２に示すように、トランザクション認証システム５０１では、例えば、発注者３１の発注者端末装置５１１と、受注者３３の受注者端末装置５１５と、ネットワーク銀行５４０の認証装置５５０と、認証履歴を格納する認証履歴格納装置１４とが、インターネットなどの外部ネットワーク（通信網）５０９を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置５５０で認証する。

なお、当該外部ネットワーク５０９に接続されているホームネットワークシステム（発注者端末システム）１０および受注者端末装置５１５の数は任意である。

本実施形態では、発注者３１の個人ＩＤ情報および個人キー情報は、受注者３３には送られない。

本実施形態は、第２２～２４の発明に対応した実施形態である。

本実施形態では、ホームネットワークシステム５１０が本発明の通信制御装置に対応し、端末装置５１１、～５１１４が本発明の第１の通信装置に対応し、認証装置５５０が本発明の第２の通信装置に対応している。

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行５４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行５４２との間では、例えば、ネットワーク銀行５４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行５４０と保険会社５４３との間では、ネットワーク銀行５４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

以下、トランザクション認証システム５０１を構成する各装置について説明する。

〔ホームネットワークシステム 510〕

図 42 および図 43 に示すように、ホームネットワークシステム 510 は、発注者 31 の各家庭などに構築されており、ホームネットワークシステム 510 のホームゲートウェイ 512 が、図 42 に示す受注者端末装置 515 および認証装置 550 が接続される外部ネットワーク 509 に有線あるいは無線で接続されている。

また、ホームゲートウェイ 512 には、例えば、家庭内の内部ネットワーク 13 を介して、端末装置 511₁、511₂、511₃、511₄ が有線あるいは無線で接続される。

端末装置 511₁～511₄ は、例えば、デジタルテレビ受信装置、パーソナルコンピュータ、電話機およびゲーム機などである。

端末装置 511₁～511₄ の各々には、例えば製造元で当該端末装置を識別するための装置 ID 情報が割り当てられており、当該装置 ID 情報が各端末装置の内部メモリに記憶されている。例えば、端末装置 511₁ には装置 ID 情報 ID_{M1} が割り当てられ、端末装置 511₂ には装置 ID 情報 ID_{M2} が割り当てられ、端末装置 511₃ には装置 ID 情報 ID_{M3} が割り当てられ、端末装置 511₄ には装置 ID 情報 ID_{M4} が割り当てられている。

図 44 は、ホームゲートウェイ 512 の構成図である。

ホームゲートウェイ 512 は、例えば、外部ネットワーク I/F 561、内部ネットワーク I/F 562、暗号化部 563、復号部 564、記憶部 565、制御部 566 および署名検証部 567 を有する。

ここで、外部ネットワーク I/F 561 および内部ネットワーク I/F 562 が、第 22 の発明の送信手段および受信手段、並びに第 23 の発明の第 1 の送信手段および第 2 の受信手段に対応している。また、記憶部 565 が、第 22 の発明の記憶手段および第 23 の発明の第 1 の記憶手段に対応している。また、制御部 566 が第 22 の発明および第 23 の発明の制御手段に対応している。

外部ネットワーク I/F 561 は、外部ネットワーク 509 を介して認証装置 550 との間で、情報あるいは要求の送受信を行なう。

内部ネットワーク I/F 562 は、内部ネットワーク 13 を介して端末装置 511₁ ~ 511₄ との間で、情報あるいは要求の送受信を行なう。

暗号化部 563 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 564 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 565 は、例えば、ホームゲートウェイ 512 の電源が投入されたときに電源がオンになっている端末装置 511₁ ~ 511₄ から内部ネットワーク 13 を介して受信した装置 ID 情報 ID_{M1} ~ ID_{M4} を記憶している。

また、記憶部 565 は、発注者 31 が作成した秘密鍵 K_{31,s}などを格納する。

署名検証部 567 は、例えば、認証装置 550 が作成した署名情報を、ネットワーク銀行 540 の公開鍵 K_{40,p}を用いて検証する。

制御部 566 は、発注者端末装置 511 内の各構成要素の処理を統括的に制御する。

制御部 566 は、ホームゲートウェイ 512 を介した端末装置 511₁ ~ 511₄ と認証装置 550 との間の通信の履歴を示す履歴情報を生成し、これを記憶部 565 に記憶する。

そのため、記憶部 565 に記憶された履歴情報にアクセスを行うだけで、家庭内に設けられた端末装置 511₁ ~ 511₄ を用いた通信の履歴を簡単に知ることができ、管理が容易になる。

また、制御部 566 は、例えば、待機状態（スタンバイ状態）になっている端末装置 511₁ ~ 511₄ に対してのアクセスを、外部ネットワーク 509 を介して受けた場合に、対応する端末装置 511₁ ~ 511₄ が動作状態になるように制御する。

制御部 566 は、例えば、発注者 31 による操作に応じて端末装置 511₁ ～ 511₄ から内部ネットワーク I/F 562 が受信した、発注情報 a1 と、個人キー情報 k1 と（本発明の個人識別情報）、個人 ID 情報 ID1（本発明の個人識別情報）と、装置 ID 情報 ID_{M1} ～ ID_{M4}（本発明の装置識別情報）との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf1 を生成する。

また、制御部 566 は、例えば、認証要求 Inf1 を認証装置 550 に送信した後に、認証装置 550 から認証応答 Inf4 を受信したときに、認証応答 Inf4 に含まれる認証要求の送信元の装置を示す装置 ID 情報と、記憶部 565 から読み出した装置 ID 情報 ID_{M1} ～ ID_{M4} の何れかが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置 515 および認証装置 550 の少なくとも一方に通知する。

〔受注者端末装置 515〕

図 45 に示すように、受注者端末装置 515 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 33 が使用するサーバ装置であり、受信部 571、送信部 572、暗号化部 573、復号部 574、記憶部 575、制御部 576 および署名検証部 577 を有する。

受信部 571 は、外部ネットワーク 509 を介して認証装置 550 から情報あるいは要求を受信する。

送信部 572 は、外部ネットワーク 509 を介して認証装置 550 に情報あるいは要求を送信する。

また、受信部 571 および送信部 572 は、発注者端末装置 511 からのアクセスに応じて、例えば、記憶部 575 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 511 に送信する。

暗号化部 573 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 574 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 575 は、受注者 33 が作成した秘密鍵 $K_{33,s}$ などを格納する。

制御部 576 は、受注者端末装置 515 内の各構成要素の処理を統括的に制御する。

署名検証部 577 は、例えば、ネットワーク銀行 540 の公開鍵 $K_{40,p}$ を用いて、認証装置 550 が作成した署名情報の検証を行う。

〔認証装置 550〕

図 46 に示すように、認証装置 550 は、受信部 581、送信部 582、暗号化部 583、復号部 584、記憶部 585、制御部 586、署名作成部 587 および課金処理部 588 を有する。

ここで、受信部 581 が第 23 の発明の第 2 の受信手段に対応し、送信部 582 が第 23 の発明の第 2 の送信手段に対応し、記憶部 585 が第 23 の発明の第 2 の記憶手段に対応し、制御部 586 が第 23 の発明の処理手段に対応している。

受信部 581 は、外部ネットワーク 509 を介してホームゲートウェイ 512 および受注者端末装置 515 から情報あるいは要求を受信する。

送信部 582 は、外部ネットワーク 509 を介してホームゲートウェイ 512 および受注者端末装置 515 に情報あるいは要求を送信する。

暗号化部 583 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 584 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 585 は、発注者 31 がネットワーク銀行 540 と契約したときに、発注者 31 の個人キー情報 k_1 と、個人 ID 情報 ID_1 と、ホームゲートウェイ 512 のアドレスとの対応表を記憶する。また、記憶部 585 は、例えば、発注者 31 および受注者 33 がネットワーク銀行 540 と契約をしたときに、発注者 31 が作成した秘密鍵 $K_{31,s}$ に対応する公開鍵 $K_{31,p}$ 、並びに受注者 33 が作成し

た秘密鍵 $K_{33, s}$ に対応する公開鍵 $K_{33, p}$ などを格納する。

制御部 586 は、認証装置 550 内の各構成要素の処理を統括的に制御する。

署名作成部 587 は、ネットワーク銀行 540 の秘密鍵 $K_{40, s}$ を用いて署名情報の作成を行う。

課金処理部 588 は、発注者 31 による取り引きに関する認証に対しての課金処理を行う。

認証装置 550 の各構成要素の詳細な処理については、後述する動作例で記載する。

以下、トランザクション認証システム 501 の動作例を説明する。

当該動作例では、図 42 に示す発注者 31 が図 43 に示す端末装置 511₁ を操作して、受注者 33 が提供する商品またはサービスの発注を行なう場合を説明する。

なお、当該動作例を開始する前提として、以下の手続および処理が行なわれている。

すなわち、発注者 31 とネットワーク銀行 540 との間で所定の契約が結ばれ、ネットワーク銀行 540 は、発注者 31 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行する。

ネットワーク銀行 540 は、個人キー情報 k_1 と、個人 ID 情報 ID_1 と、ホームゲートウェイ 512 のアドレスとの対応表を図 46 に示す認証装置 550 の記憶部 585 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 540 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行 540 は、自らの秘密鍵 $K_{40, s}$ を図 46 に示す認証装置 550 の記憶部 585 に記憶すると共に、当該秘密鍵 $K_{40, s}$ に対応する公開鍵

$K_{40, P}$ をホームゲートウェイ 5 1 2 および受注者端末装置 5 1 5 に送信する。ホームゲートウェイ 5 1 2 は、公開鍵 $K_{40, P}$ を図 4 4 に示す記憶部 5 6 5 に記憶する。受注者端末装置 5 1 5 は、公開鍵 $K_{40, P}$ を図 4 5 に示す記憶部 5 7 5 に記憶する。

また、受注者 3 3 とネットワーク銀行 5 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 5 4 0 は、受注者 3 3 に対して、受注者 3 3 を特定する情報 Z および個人 ID 情報 ID_2 を発行する。ネットワーク銀行 5 4 0 は、個人キー情報 Z および個人 ID 情報 ID_2 の対応表を図 4 6 に示す認証装置 5 5 0 の記憶部 5 8 5 に記憶する。

また、ホームゲートウェイ 5 1 2 の電源が投入されたときに電源がオンになっている端末装置 5 1 1₁ ~ 5 1 1₄ から内部ネットワーク 1 3 を介してホームゲートウェイ 5 1 2 が受信した装置 ID 情報 ID_{M1} ~ ID_{M4} が、図 4 4 に示す記憶部 5 6 5 に記憶される。

図 4 7 A ~ 4 7 F は、トランザクション認証システム 5 0 1 の動作例を説明するための図である。

ステップ S T 6 1 :

図 4 2 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a_1 と、発注者 3 1 の個人キー情報 k_1 と、発注者 3 1 の個人 ID 情報 ID_1 とを、図示しない操作手段を操作して端末装置 5 1 1₁ に入力する。なお、発注情報 a_1 には、受注者 3 3 を特定する情報が含まれている。

端末装置 5 1 1₁ は、当該入力された発注情報 a_1 と、発注者 3 1 の個人キー情報 k_1 と、発注者 3 1 の個人 ID 情報 ID_1 と、内部メモリから読み出した装置 ID 情報 ID_{M1} とを、内部ネットワーク 1 3 を介して、ホームゲートウェイ 5 1 2 に送信する。

ステップ S T 6 2 :

図 4 4 に示すホームゲートウェイ 5 1 2 は、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、装置 ID 情報 ID_{M1}とを内部ネットワーク I/F 5 6 2 で受信し、これらの全体に対して暗号化部 5 6 3 で暗号化を行う。

ホームゲートウェイ 5 1 2 は、当該暗号化した情報を格納した認証要求 Inf 1（本発明の要求）を、図 4 4 に示す外部ネットワーク I/F 5 6 1 から外部ネットワーク 5 0 9 を介して、図 4 2 に示すネットワーク銀行 5 4 0 の認証装置 5 5 0 に送信する。

ステップ ST 6 3 :

図 4 6 に示す認証装置 5 5 0 は、ホームゲートウェイ 5 1 2 からの認証要求 Inf 1 を受信部 5 8 1 が受信すると、記憶部 5 8 5 からネットワーク銀行 5 4 0 の秘密鍵 K_{40, s}を読み出し、復号部 5 8 4 において、当該秘密鍵 K_{40, s}を用いて認証要求 Inf 1 を復号する。

次に、認証装置 5 5 0 は、制御部 5 8 6 の制御に基づいて、上記復号した認証要求 Inf 1 から個人キー情報 k 1 および個人 ID 情報 ID 1 を削除した情報 Inf 1' について、記憶部 5 8 5 から読み出した自らの秘密鍵 K_{40, s}を用いて署名情報 Au 1 を作成する。

次に、認証装置 5 5 0 は、情報 Inf 1' および署名情報 Au 1 を格納した要求 Inf 2 を生成する。

次に、暗号化部 5 8 3 は、図 4 6 に示す記憶部 5 8 5 から読み出した受注者 3 の公開鍵 K_{33, P}を用いて、上記生成した要求 Inf 2 を暗号化した後に、送信部 5 8 2 から、外部ネットワーク 5 0 9 を介して受注者端末装置 5 1 5 に送信する。

ステップ ST 6 4 :

受注者端末装置 5 1 5 の復号部 5 7 4 は、認証装置 5 5 0 からの要求 Inf 2 を受信部 5 7 1 が受信すると、記憶部 5 7 5 から読み出した自らの秘密鍵 K_{33, s}を用いて、要求 Inf 2 を復号する。

次に、受注者端末装置 5 1 5 の署名検証部 5 7 7 は、上記復号した要求 I n f 2 に格納された署名情報 A u 1 を、記憶部 5 7 5 から読み出した認証装置 5 5 0 の公開鍵 $K_{40, P}$ を用いて検証する。

受注者端末装置 5 1 5 の制御部 5 7 6 は、署名検証部が上記検証の結果、署名情報 A u 1 の正当性が認証されると、要求 I n f 2 に格納された情報 I n f 1' を図 4 5 に示す記憶部 5 7 5 に記憶する。受注者 3 3 は、情報 I n f 1' 内の発注情報 a 1 に基づいて、発注者 3 1 への商品等の発送予定などを示す受注確認情報 c 1 を生成する。

次に、制御部 5 7 6 は、要求 I n f 2、受注確認情報 c 1 および自らを特定する情報 Z を格納した応答 I n f 3 を生成する。

次に、受注者端末装置 5 1 5 の送信部 5 7 2 は、上記生成した応答 I n f 3 を、記憶部 5 7 5 から読み出したネットワーク銀行 5 4 0 の公開鍵 $K_{40, P}$ を用いて暗号化部 5 7 3 で暗号化した後に、送信部 5 7 2 から、外部ネットワーク 5 0 9 を介して認証装置 5 5 0 に送信する。

受注者 3 3 は、例えば、要求 I n f 2 に格納された情報 I n f 1' 内の発注情報 a 1 に基づいて、発注者 3 1 が発注した商品等を発注者 3 1 に発送したり、発注者 3 1 が注文したサービスを発注者 3 1 に提供する。

ステップ S T 6 5 :

認証装置 5 5 0 の復号部 5 8 4 は、受注者端末装置 5 1 5 からの応答 I n f 3 を受信部 5 8 1 が受信すると、記憶部 5 8 5 から読み出した自らの秘密鍵 $K_{40, S}$ を用いて、I n f 3 を復号し、要求 I n f 1 に格納された発注情報 a 1 と、当該復号された I n f 3 に格納された受注者 3 3 の情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 5 8 5 に格納する。当該履歴情報は、ネットワーク銀行 5 4 0 が、発注者 3 1 に対して決済を行う際に用いられる。

また、認証装置 5 5 0 の署名作成部 5 8 7 は、ステップ S T 6 4 で受信した応答 I n f 3 について、自らの秘密鍵 $K_{40, S}$ を用いて署名情報 A u 2 を作成する。

次に、認証装置 550 の制御部 586 は、応答 $I n f 3$ および署名情報 $A u 2$ を格納した認証応答 $I n f 4$ を作成する。

次に、認証装置 550 の暗号化部 583 は、上記作成した認証応答 $I n f 4$ を、記憶部 585 から読み出した発注者 31 の公開鍵 $K_{31, P}$ を用いて暗号化する。

そして、図 46 に示す記憶部 585 に個人 ID 情報 $I D 1$ と対応して記憶されているホームゲートウェイ 512 のアドレスを用いて、送信部 582 から外部ネットワーク 509 を介してホームゲートウェイ 512 に当該暗号化した応答 $I n f 4$ を送信する。

ホームゲートウェイ 512 では、受信した認証応答 $I n f 4$ を、図 44 示す記憶部 565 から読み出した発注者 31 の秘密鍵 $K_{31, S}$ を用いて復号部 564 で復号する。

次に、ホームゲートウェイ 512 の署名検証部 566 は、当該復号した認証応答 $I n f 4$ に格納された署名情報 $A u 2$ を、記憶部 565 から読み出したネットワーク銀行 540 の公開鍵 $K_{40, P}$ を用いて検証すると共に、 $I n f 4$ 内の発注情報 $a 1$ 内に記述された装置 ID 情報 $I D_{M1}$ が図 44 に示す記憶部 565 に記憶されている装置 ID 情報 $I D_{M1} \sim I D_{M4}$ の何れかと一致するか否かを判断する。当該動作例では、一致すると判断され、発注者 31 と受注者 33 との間の当該取引引きが正当に行われたことが確認される。

ステップ S T 66 :

ホームゲートウェイ 512 は、応答 $I n f 4$ に含まれる $I n f 3$ を、内部ネットワーク 13 を介して端末装置 511₁ に送信する。

端末装置 511₁ は、当該受信した $I n f 3$ に格納された受注確認情報 $c 1$ をディスプレイなどに表示する。

以下、発注者 31 の個人 ID 1 および個人キー $k 1$ を不正に取得した図 42 に

示す不正者 5 5 が自らの端末装置である不正者端末装置 5 5 6 を用いて、認証装置 5 5 0 に認証要求を送信した場合のトランザクション認証システム 5 0 1 の動作を説明する。

図 4 8 A ~ 4 8 E は、トランザクション認証システム 5 0 1 の当該動作を説明するための図である。

ステップ S T 7 1 :

図 4 2 に示す不正者 5 5 は、受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、不正に取得した発注者 3 1 の個人情報 k 1 と、不正に取得した発注者 3 1 の個人 I D 情報 I D 1 とを、図示しない操作手段を操作して不正者端末装置 5 5 6 に入力する。

不正者端末装置 5 5 6 は、発注情報 a 1 と、個人情報 k 1 と、個人 I D 情報 I D 1 と、内部メモリから読み出した装置 I D 情報 I D_{M56} を暗号化し、当該暗号化した情報を格納した認証要求 I n f 1 を、外部ネットワーク 5 0 9 を介して、図 4 2 に示すネットワーク銀行 5 4 0 の認証装置 5 5 0 に送信する。

図 4 6 に示す認証装置 5 5 0 は、不正者端末装置 5 5 6 からの認証要求 I n f 1 を受信部 5 8 1 が受信すると、当該認証要求 I n f 1 について、前述したステップ S T 6 2 と同様の処理を行なう。

ステップ S T 7 2 :

ステップ S T 7 2 の処理は、前述したステップ S T 6 3 の処理と同じである。

ステップ S T 7 3 :

ステップ S T 7 3 の処理は、前述したステップ S T 6 4 の処理と同じである。

ステップ S T 7 4 :

ステップ S T 7 4 の処理は、前述したステップ S T 6 5 の処理と同じである。

ステップ S T 7 5 :

ステップ S T 7 5 の処理は、前述したステップ S T 6 6 の処理と同じである。

このように、トランザクション認証システム 5 0 1 によれば、不正者 5 5 が不

正者端末装置 556 を用いて、認証要求 Inf 1 を認証装置 550 に送信した場合でも、その応答である認証応答 Inf 4 は、認証装置 550 の記憶部 585 に個人 ID 情報 ID 1 と対応して記憶されているホームゲートウェイ 512 のアドレスに基づいて、ホームゲートウェイ 512 に送信される。

これにより、ホームゲートウェイ 512 において、認証応答 Inf 4 に含まれる装置 ID 情報 ID_{M56} が、図 44 に示す記憶部 565 に記憶されている装置 ID 情報 ID_{M1} ~ ID_{M4} と一致しないと判断され、発注者 31 の個人 ID 情報 ID 1 を用いた不正な認証要求が行なわれたことを検出できる。

そのため、トランザクション認証システム 501 によれば、他人の個人 ID 情報を用いた不正な取り引きを効果的に抑制できる。

上述したように、トランザクション認証システム 501 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

また、トランザクション認証システム 501 によれば、例えば、図 42 および図 43 に示す端末装置 511_i からの要求に応じて認証要求 Inf 1 を認証装置 550 に送信した後に、端末装置 511_i が故障した場合でも、当該認証要求 Inf 1 に応じた認証応答 Inf 4 に応じた処理を適切に行うことができる。

また、トランザクション認証システム 501 によれば、外部ネットワーク 509 を介した通信に伴うセキュリティに関する機能をホームゲートウェイ 512 に持たせることで、端末装置 511_i ~ 11₄ に備えるセキュリティ機能のレベルを下げることができ、端末装置 511_i ~ 11₄ の構成を簡単かつ安価にできる。

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の第 2 の通信装置として認証処理を行う認証装置 550 を例示したが、第 2 の通信装置が行う処理はその他、課金処理

などであってもよい。

また、上述した実施形態では、ネットワーク銀行 540 が、認証装置 550 を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行 540 とは別の機関が、認証装置 550 を用いてトランザクションの認証業務を行うようにしてもよい。

また、上述した実施形態では、端末装置 511₁ ～ 511₄ の装置 ID 情報を認証装置 550 に送信した場合を例示したが、ホームゲートウェイ 512 の装置 ID 情報を認証装置 550 に送信するようにしてもよい。

第 9 実施形態

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図 49 は、本実施形態のトランザクション認証システム 201 の全体構成図である。

図 49 に示すように、トランザクション認証システム 201 では、例えば、発注者 31 の発注者端末装置 211 と、受注者 33 の受注者端末装置 215 と、ネットワーク銀行 240 の認証装置 250 と、認証履歴を格納する認証履歴格納装置 14 とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者 31 と受注者 33 との間のトランザクション（取引）の正当性を認証装置 250 で認証する。

なお、当該ネットワークに接続されている発注者端末装置 211 および発注者受注者端末装置 215 の数は任意である。

本実施形態では、発注者 31 の個人 ID 情報および個人キー情報は、受注者 33 には送られない。

本実施形態は、第 25 ～ 第 29 の発明に対応した実施形態である。

発注者端末装置 211 が第 27 の発明の処理装置に対応し、認証装置 250 が本発明の認証装置に対応している。

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 2 4 0 との間で認証を行うことについての契約が成されている。また、発注者 3 1 と引き落とし銀行 2 4 2 との間では、例えば、ネットワーク銀行 2 4 0 によって認証された取引に関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 2 4 0 と保険会社 2 4 3 との間では、ネットワーク銀行 2 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

以下、トランザクション認証システム 2 0 1 を構成する各装置について説明する。

〔発注者端末装置 2 1 1〕

図 5 0 に示すように、発注者端末装置 2 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 2 6 1、送信部 2 6 2、暗号化部 2 6 3、復号部 2 6 4、記憶部 2 6 5、制御部 2 6 6 および署名検証部 2 6 7 を有する。

なお、発注者端末装置 2 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 2 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な利用者であることを認証する生体認証部を有していてもよい。

ここで、受信部 2 6 1 が第 2 7 の発明の受信手段に対応し、送信部 2 6 2 が第 2 7 の発明の送信手段に対応し、制御部 2 6 6 が第 2 7 の発明の制御手段に対応している。

受信部 2 6 1 は、ネットワークを介して認証装置 2 5 0 から情報あるいは要求を受信する。

送信部 2 6 2 は、ネットワークを介して認証装置 2 5 0 に情報あるいは要求を送信する。

また、受信部 261 および送信部 262 は、受注者 33 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 263 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 264 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 265 は、製造元で受注者端末装置 215 に付された装置 ID 情報 ID_M （本発明の装置識別情報）と、発注者 31 が作成した秘密鍵 $K_{33,s}$ などを格納する。

署名検証部 267 は、例えば、認証装置 250 が作成した署名情報を、ネットワーク銀行 240 の公開鍵 $K_{40,p}$ を用いて検証する。

制御部 266 は、発注者端末装置 211 内の各構成要素の処理を統括的に制御する。

制御部 266 は、例えば、発注者 31 による操作に応じて、発注情報 a_1 と、個人キー情報 k_1 （本発明の個人識別情報）と、個人 ID 情報 ID_1 （本発明の個人識別情報）と、記憶部 265 から読み出した装置 ID 情報 ID_M との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf_1 を生成する。

また、制御部 266 は、例えば、認証要求 Inf_1 を認証装置 250 に送信した後に、認証装置 250 から認証応答 Inf_4 を受信したときに、認証応答 Inf_4 に含まれる認証要求の送信元の装置を示す装置 ID 情報 ID_M と、記憶部 265 から読み出した発注者端末装置 211 の装置 ID 情報 ID_M とが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置 215 および認証装置 250 の少なくとも一方に通知する。

〔受注者端末装置 215〕

図 5 1 に示すように、受注者端末装置 2 1 5 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 2 7 1、送信部 2 7 2、暗号化部 2 7 3、復号部 2 7 4、記憶部 2 7 5、制御部 2 7 6 および署名検証部 2 7 7 を有する。

受信部 2 7 1 は、ネットワークを介して認証装置 2 5 0 から情報あるいは要求を受信する。

送信部 2 7 2 は、ネットワークを介して認証装置 2 5 0 に情報あるいは要求を送信する。

また、受信部 2 7 1 および送信部 2 7 2 は、発注者端末装置 2 1 1 からのアクセスに応じて、例えば、記憶部 2 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 2 1 1 に送信する。

暗号化部 2 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 2 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 2 7 5 は、受注者 3 3 が作成した秘密鍵 $K_{33, s}$ などを格納する。

制御部 2 7 6 は、受注者端末装置 2 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 2 7 7 は、例えば、ネットワーク銀行 2 4 0 の公開鍵 $K_{40, p}$ を用いて、認証装置 2 5 0 が作成した署名情報の検証を行う。

〔認証装置 2 5 0〕

図 5 2 に示すように、認証装置 2 5 0 は、受信部 2 8 1、送信部 2 8 2、暗号化部 2 8 3、復号部 2 8 4、記憶部 2 8 5、制御部 2 8 6、署名作成部 2 8 7 および課金処理部 2 8 8 を有する。

ここで、受信部 2 8 1 が第 2 5 および第 2 6 の発明の受信手段に対応し、送信部 2 8 2 が第 2 5 および第 2 6 の発明の送信手段に対応し、記憶部 2 8 5 が第 2 5 および第 2 6 の発明の記憶手段に対応し、制御部 2 8 6 が第 2 5 および第 2 6

の発明の認証処理手段に対応している。

受信部 281 は、ネットワークを介して発注者端末装置 211 および受注者端末装置 215 から情報あるいは要求を受信する。

送信部 282 は、ネットワークを介して発注者端末装置 211 および受注者端末装置 215 に情報あるいは要求を送信する。

暗号化部 283 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 284 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 285 は、発注者 31 がネットワーク銀行 240 と契約したときに、発注者 31 の個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者端末装置 211 のアドレス（または、発注者端末装置 211 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を記憶する。また、記憶部 285 は、例えば、発注者 31 および受注者 33 がネットワーク銀行 240 と契約をしたときに、発注者 31 が作成した秘密鍵 $K_{31,s}$ に対応する公開鍵 $K_{31,p}$ 、並びに受注者 33 が作成した秘密鍵 $K_{33,s}$ に対応する公開鍵 $K_{33,p}$ などを格納する。

制御部 286 は、認証装置 250 内の各構成要素の処理を統括的に制御する。

署名作成部 287 は、ネットワーク銀行 240 の秘密鍵 $K_{40,s}$ を用いて署名情報の作成を行う。

課金処理部 288 は、発注者 31 による取引に関する認証に対しての課金処理を行う。

認証装置 250 の各構成要素の詳細な処理については、後述する動作例で記載する。

以下、トランザクション認証システム 201 の動作例を説明する。

当該動作例を開始する前提として、発注者 31 とネットワーク銀行 240 との

間で所定の契約が結ばれ、ネットワーク銀行 240 は、発注者 31 に対して、個人キー情報 k_1 および個人 ID 情報 ID1 を発行する。

ネットワーク銀行 240 は、個人キー情報 k_1 と、個人 ID 情報 ID1 と、発注者端末装置 211 のアドレス（または、発注者端末装置 211 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を図 52 に示す認証装置 250 の記憶部 285 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 240 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID1 は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行 240 は、自らの秘密鍵 $K_{40,s}$ を図 52 に示す認証装置 250 の記憶部 285 に記憶すると共に、当該秘密鍵 $K_{40,s}$ に対応する公開鍵 $K_{40,p}$ を発注者端末装置 211 および受注者端末装置 215 に送信する。発注者端末装置 211 は、公開鍵 $K_{40,p}$ を図 50 に示す記憶部 265 に記憶する。受注者端末装置 215 は、公開鍵 $K_{40,p}$ を図 51 に示す記憶部 275 に記憶する。

また、受注者 33 とネットワーク銀行 240 との間で所定の契約が結ばれ、ネットワーク銀行 240 は、受注者 33 に対して、受注者 33 を特定する情報 Z および個人 ID 情報 ID2 を発行する。ネットワーク銀行 240 は、情報 Z および個人 ID 情報 ID2 の対応表を図 52 に示す認証装置 250 の記憶部 285 に記憶する。

図 53A～53E は、トランザクション認証システム 201 の動作例を説明するための図である。

ステップ ST21 :

図 49 に示す発注者 31 は、例えばネットワーク上の商店である受注者 33 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a_1 と、発注者 31 の個人キー情報 k_1 と、発注者 31 の個人 ID 情報 ID1 とを、図示しない操作手段を操作して発注者端末装置 211 に入力する。なお、発注情報 a

1 には、受注者 3 3 を特定する情報が含まれている。

次に、図 5 0 に示す発注者端末装置 2 1 1 の暗号化部 2 6 3 は、記憶部 2 6 5 から読み出したネットワーク銀行 2 4 0 の公開鍵 $K_{40, P}$ を用いて、発注情報 $a 1$ と、個人キー情報 $k 1$ と、個人 ID 情報 $ID 1$ と、記憶部 2 6 5 から読み出した装置 ID 情報 ID_M との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 $I n f 1$ (本発明の第 1 の要求) を、送信部 2 6 2 からネットワークを介して、図 4 9 に示すネットワーク銀行 2 4 0 の認証装置 2 5 0 に送信する。

ステップ S T 2 2 :

図 5 2 に示す認証装置 2 5 0 は、発注者端末装置 2 1 1 からの認証要求 $I n f 1$ を受信部 2 8 1 が受信すると、記憶部 2 8 5 からネットワーク銀行 2 4 0 の秘密鍵 $K_{40, s}$ を読み出し、復号部 2 8 4 において、当該秘密鍵 $K_{40, s}$ を用いて認証要求 $I n f 1$ を復号する。

次に、認証装置 2 5 0 は、制御部 2 8 6 の制御に基づいて、上記復号した認証要求 $I n f 1$ から個人キー情報 $k 1$ および個人 ID 情報 $ID 1$ を削除した情報 $I n f 1'$ について、記憶部 2 8 5 から読み出した自らの秘密鍵 $K_{40, s}$ を用いて署名情報 $A u 1$ を作成する。

次に、認証装置 2 5 0 は、情報 $I n f 1'$ および署名情報 $A u 1$ を格納した要求 $I n f 2$ を生成する。

次に、暗号化部 2 8 3 は、図 5 2 に示す記憶部 2 8 5 から読み出した受注者 3 3 の公開鍵 $K_{33, P}$ を用いて、上記生成した要求 $I n f 2$ を暗号化した後に、送信部 2 8 2 から、ネットワークを介して受注者端末装置 2 1 5 に送信する。

ステップ S T 2 3 :

受注者端末装置 2 1 5 の復号部 2 7 4 は、認証装置 2 5 0 からの要求 $I n f 2$ を受信部 2 7 1 が受信すると、記憶部 2 7 5 から読み出した自らの秘密鍵 $K_{33, s}$ を用いて、要求 $I n f 2$ を復号する。

次に、受注者端末装置 2 1 5 の署名検証部 2 7 7 は、上記復号した要求 I n f 2 に格納された署名情報 A u 1 を、記憶部 2 7 5 から読み出した認証装置 2 5 0 の公開鍵 $K_{40, P}$ を用いて検証する。

受注者端末装置 2 1 5 の制御部 2 7 6 は、署名検証部が上記検証の結果、署名情報 A u 1 の正当性が認証されると、要求 I n f 2 に格納された情報 I n f 1 ' を図 5 1 に示す記憶部 2 7 5 に記憶する。受注者 3 3 は、情報 I n f 1 ' 内の発注情報 a 1 に基づいて、発注者 3 1 への商品等の発送予定などを示す受注確認情報 c 1 を生成する。

次に、制御部 2 7 6 は、要求 I n f 2、受注確認情報 c 1 および自らを特定する情報 Z を格納した応答 I n f 3 を生成する。

次に、受注者端末装置 2 1 5 の送信部 2 7 2 は、上記生成した応答 I n f 3 を、記憶部 2 7 5 から読み出したネットワーク銀行 2 4 0 の公開鍵 $K_{40, P}$ を用いて暗号化部 2 7 3 で暗号化した後に、送信部 2 7 2 から、ネットワークを介して認証装置 2 5 0 に送信する。

受注者 3 3 は、例えば、要求 I n f 2 に格納された情報 I n f 1 ' 内の発注情報 a 1 に基づいて、発注者 3 1 が発注した商品等を発注者 3 1 に発送したり、発注者 3 1 が注文したサービスを発注者 3 1 に提供する。

ステップ S T 2 4 :

認証装置 2 5 0 の復号部 2 8 4 は、受注者端末装置 2 1 5 からの応答 I n f 3 を受信部 2 8 1 が受信すると、記憶部 2 8 5 から読み出した自らの秘密鍵 $K_{40, S}$ を用いて、I n f 3 を復号し、要求 I n f 1 に格納された発注情報 a 1 と、当該復号された I n f 3 に格納された受注者 3 3 の情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 2 8 5 に格納する。当該履歴情報は、ネットワーク銀行 2 4 0 が、発注者 3 1 に対して決済を行う際に用いられる。

また、認証装置 2 5 0 の署名作成部 2 8 7 は、ステップ S T 2 3 で受信した応答 I n f 3 について、自らの秘密鍵 $K_{40, S}$ を用いて署名情報 A u 2 を作成する。

次に、認証装置 250 の制御部 286 は、応答 Inf 3 および署名情報 Au 2 を格納した認証応答 Inf 4 を作成する。

次に、認証装置 250 の暗号化部 283 は、上記作成し認証した応答 Inf 4 を、記憶部 285 から読み出した発注者 31 の公開鍵 $K_{31,P}$ を用いて暗号化した後に、送信部 282 から、ネットワークを介して発注者端末装置 211 に送信する。

ステップ ST 25 :

発注者端末装置 211 では、受信した認証応答 Inf 4 を、図 50 示す記憶部 265 から読み出した発注者 31 の秘密鍵 $K_{31,S}$ を用いて復号部 264 で復号する。

次に、発注者端末装置 211 の署名検証部 266 は、当該復号した認証応答 Inf 4 に格納された署名情報 Au 2 を、記憶部 265 から読み出したネットワーク銀行 240 の公開鍵 $K_{40,P}$ を用いて検証すると共に、Inf 4 内の発注情報 a1 内に記述された装置 ID 情報 ID_M が図 50 に示す発注者端末装置 211 の記憶部 265 に記憶されている自らの装置 ID 情報 ID_M と一致するかを判断し、一致すると判断した場合には、受注者 33 との間の当該取り引きが正当に行われたことを確認する。発注者端末装置 211 は、Inf 4 内の発注情報 a1 内に記述された装置 ID 情報 ID_M が図 50 に示す発注者端末装置 211 の記憶部 265 に記憶されている自らの装置 ID 情報 ID_M と一致しないと判断した場合には、例えば、認証応答 Inf 4 を格納した不正発注通知 Inf 5 を認証装置 250 および受注者端末装置 215 の少なくとも一方に送信する。

これにより、認証装置 250 および受注者端末装置 215 は、発注者端末装置 211 が発した認証要求 Inf 1 に対応した発注を取り消す。

また、発注者端末装置 211 は、不正発生通知 Inf 5 を、図 49 に示す引き落とし銀行 242 に送信してもよい。

以上説明したように、トランザクション認証システム 201 によれば、認証要求 Inf 1 内に、個人 ID 情報 ID 1 の他に当該認証要求を出した装置 ID 情報 ID_M を自動的に挿入し、認証装置 250 において、認証要求 Inf 1 に含まれる発注者 31 が使用する発注者端末装置 211 のアドレスに、認証結果を含む認証応答 Inf 4 を送信し、当該認証応答 Inf 4 内に当該認証要求を出した装置 ID 情報 ID_M を格納することで、発注者端末装置 211 では、認証応答 Inf 4 に格納された当該認証要求を出した装置 ID 情報 ID_M と自らの装置 ID 情報 ID_M とが一致するか否かを判断することで、自らの個人 ID 情報 ID 1 を用いた不正な認証要求（なりすまし）が発生したことを検出できる。

その結果、トランザクション認証システム 201 によれば、他人の個人 ID 情報を用いた不正な取り引きを効果的に抑制できる。

上述したように、トランザクション認証システム 1201 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、発注者端末装置 211 において、認証応答 Inf 4 内の発注情報 a 1 内に記述された装置 ID 情報 ID_M が図 50 に示す発注者端末装置 211 の記憶部 265 に記憶されている自らの装置 ID 情報 ID_M と一致するかを判断し、一致しないと判断した場合には、例えば、認証応答 Inf 4 を格納した不正発注通知 Inf 5 を認証装置 250 および受注者端末装置 215 の少なくとも一方に送信する場合を例示したが、例えば、一致しない旨（不正な取り引きが行われた旨）を発注者端末装置 211 のディスプレイなどに表示し、発注者 31 にその旨を知らせるようにしてもよい。

また、発注者端末装置 211 において、上述した装置 ID 情報 ID_M の一致を判断するのではなく、発注者 31 が判断してもよい。

また、発注者端末装置 2 1 1 が配設された家庭にホーム・ゲートウェイ (Home Gateway) が設置されている場合には、ホーム・ゲートウェイに発注者端末装置 2 1 1 の装置 ID 情報 ID_M を登録しておき、認証装置 2 5 0 からの認証応答 Inf 4 をホーム・ゲートウェイが受信したときに、ホーム・ゲート・ウェイにおいて、上記装置 ID 情報 ID_M の一致の判断を行ってもよい。

また、上述した実施形態では、ネットワーク銀行 2 4 0 が、認証装置 2 5 0 を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行 2 4 0 とは別の機関が、認証装置 2 5 0 を用いてトランザクションの認証業務を行うようにしてもよい。

また、上述した実施形態では、図 5 3 A に示すステップ ST 2 1 のように、暗号化された発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、装置 ID 情報 ID_M とを含む認証要求 Inf 1 を、発注者端末装置 2 1 1 から認証装置 2 5 0 に送信する場合を例示したが、発注情報 a 1 と、個人キー情報 k 1 と、装置 ID 情報 ID_M とを含む認証要求 Inf 1 を、発注者端末装置 2 1 1 から認証装置 2 5 0 に送信してもよい。このようにすれば、課金に係わる情報である個人 ID 情報 ID 1 はネットワークを介して伝送されないため、ネットワーク上で個人 ID 情報 ID 1 が不正に取得され、悪用されることを回避できる。

また、上述した実施形態では、図 5 0 に示す発注者端末装置 2 1 1 の暗号化部 2 6 3 において、記憶部 2 6 5 から読み出した所定の暗号鍵を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、記憶部 2 6 5 から読み出した装置 ID 情報 ID_M との全体に対して暗号化を行う場合を例示したが、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、記憶部 2 6 5 から読み出した装置 ID 情報 ID_M とのそれぞれについて個別に暗号化を行ってもよい。

第 1 0 実施形態

図 5 4 は、本実施形態の情報記録装置 6 0 1 の構成図である。

図 5 4 に示すように、情報記録装置 6 0 1 は、読み出し回路 6 1 0、暗号化回路 6 1 1、情報分割回路 6 1 2、書き込み回路 6 1 3、6 1 4 を有する。

本実施形態は、第 3 0、3 2 および 3 4 の発明に対応した実施形態である。

情報記録装置 6 0 1 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を暗号化した後に、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 3、D 4 に分割し、モジュール D 3 を記録媒体 6 1 6 に書き込み、モジュール D 4 を記録媒体 6 1 7 に書き込む。

本実施形態において、記録媒体 6 1 5、6 1 6、6 1 7 は、HDD 装置や、携帯性のある CD-ROM、フロッピーディスク、PC カードなどの記録媒体である。

読み出し回路 6 1 0 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を暗号化回路 6 1 1 に出力する。

個人情報 D 1 は、図 5 5 に示すように、情報 Data 1 ~ Data N からなる。

また、個人情報 D 1 は、例えば、ユーザの個人 ID 情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

暗号化回路 6 1 1 は、所定の暗号鍵を用いて、読み出し回路 6 1 0 から入力した個人情報 D 1 を暗号化して個人情報 D 2 を生成し、これを情報分割回路 6 1 2 に出力する。

暗号化された個人情報 D 2 は、図 5 5 に示すように、それぞれ情報 Data 1 ~ Data N を暗号化した情報 Data 1' ~ Data N' からなる。

情報分割回路 6 1 2 は、暗号化回路 6 1 1 から入力した暗号化された個人情報 D 2 を、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 3、D 4 に分割し、モジュール D 3 を書き込み回路 6 1 3 に出力し、モジュール D 4 を書き込み回路 6 1 4 に出力する。

図55に示すように、情報分割回路612は、情報D2内の情報Data1' ~ DataN' を、それぞれ情報Data1A' およびData1B'、情報Data2A' およびData2B'、情報Data3A' およびData3B'、...、情報DataKA' およびDataKB'、...、情報DataNA' およびDataNB' に分割する。

そして、情報分割回路612は、情報Data1A'、Data2A'、Data3A'、...、DataKA'、...、DataNA' からなるモジュールD3を書き込み回路613に出力する。

また、情報分割回路612は、情報Data1B'、Data2B'、Data3B'、...、DataKB'、...、DataNB' からなるモジュールD4を書き込み回路614に出力する。

書き込み回路613は、情報分割回路612から入力したモジュールD3を記録媒体616に書き込む。

書き込み回路614は、情報分割回路612から入力したモジュールD4を記録媒体617に書き込む。

以下、情報記録装置601の動作を説明する。

図56は、情報記録装置601の動作を説明するためのフローチャートである。

ステップST81:

読み出し回路610によって、記録媒体615から図55に示す個人情報D1が読み出されて暗号化回路611に出力される。

ステップST82:

暗号化回路611において、所定の暗号鍵を用いて、読み出し回路610から入力された個人情報D1が暗号化されて図55に示す個人情報D2が生成され、当該個人情報D2が情報分割回路612に出力される。

ステップST83:

情報分割回路 6 1 2 において、暗号化回路 6 1 1 から入力された個人情報 D 2 が、それぞれを単独では個人情報 D 1 の秘匿性が保持される図 5 5 に示す 2 つのモジュール D 3, D 4 に分割される。

そして、情報分割回路 6 1 2 から書き込み回路 6 1 3 にモジュール D 3 が出力され、情報分割回路 6 1 2 から書き込み回路 6 1 4 にモジュール D 4 が出力される。

ステップ S T 8 4 :

書き込み回路 6 1 3 によって、モジュール D 3 が記録媒体 6 1 6 に書き込まれる。

書き込み回路 6 1 4 によって、モジュール D 4 が記録媒体 6 1 7 に書き込まれる。

以上説明したように、情報記録装置 6 0 1 によれば、図 5 5 に示すように、個人情報 D 1 が、暗号化された後に、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 3, D 4 に分割され、モジュール D 3, D 4 がそれぞれ物理的に独立した記録媒体 6 1 6, 6 1 7 にそれぞれ記録される。

そのため、記録媒体 6 1 6, 6 1 7 を別々に保管すれば、記録媒体 6 1 6, 6 1 7 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D 1 の秘匿性は保たれる。

第 1 1 実施形態

図 5 7 は、本実施形態の情報復元装置 6 3 1 の構成図である。

情報復元装置 6 3 1 は、上述した第 4 実施形態の情報記録装置 6 0 1 によって、記録媒体 6 1 6 と 6 1 7 とに分割して記録された個人情報から、本来の個人情報 D 1 を復元する。

本実施形態は、第 3 1 および 3 3 の発明に対応した実施形態である。

図 5 7 に示すように、情報復元装置 6 3 1 は、読み出し回路 6 2 0, 6 2 1、

情報合成回路 6 2 2、復号回路 6 2 3 および書き込み回路 6 2 4 を有する。

図 5 7 において、記録媒体 6 1 6 および 6 1 7 には、前述した第 1 0 実施形態で説明した図 5 6 に示す処理を経て、それぞれモジュール D 3 および D 4 が記録されている。

読み出し回路 6 2 0 は、記録媒体 6 1 6 から読み出したモジュール D 3 を情報合成回路 6 2 2 に出力する。

読み出し回路 6 2 1 は、記録媒体 6 1 7 から読み出したモジュール D 4 を情報合成回路 6 2 2 に出力する。

情報合成回路 6 2 2 は、図 5 8 に示すように、読み出し回路 6 2 0 から入力したモジュール D 3 と、読み出し回路 6 2 1 から入力したモジュール D 4 とを合成して個人情報 D 2 を生成し、これを復号回路 6 2 3 に出力する。

復号回路 6 2 3 は、情報合成回路 6 2 2 から入力した個人情報 D 2 を、所定の復号鍵を用いて復号して個人情報 D 1 を生成し、これを書き込み回路 6 2 4 に出力する。

書き込み回路 6 2 4 は、復号回路 6 2 3 から入力した個人情報 D 1 を、記録媒体 6 1 5 に書き込む。

以下、情報復元装置 6 3 1 の動作を説明する。

図 5 9 は、情報復元装置 6 3 1 の動作を説明するためのフローチャートである。

ステップ S T 9 1 :

読み出し回路 6 2 0 によって、記録媒体 6 1 6 から図 5 8 に示すモジュール D 3 が読み出されて情報合成回路 6 2 2 に出力される。

また、読み出し回路 6 2 1 によって、記録媒体 6 1 7 から図 5 8 に示すモジュール D 4 が読み出されて情報合成回路 6 2 2 に出力される。

ステップ S T 9 2 :

情報合成回路 6 2 2 において、図 5 8 に示すように、読み出し回路 6 2 0 から

入力したモジュールD 3 と、読み出し回路6 2 1 から入力したモジュールD 4 とが合成されて個人情報D 2 が生成される。

個人情報D 2 は、情報合成回路6 2 2 から復号回路6 2 3 に出力される。

ステップS T 9 3 :

復号回路6 2 3 において、情報合成回路6 2 2 から入力した個人情報D 2 が、所定の復号鍵を用いて復号して個人情報D 1 を生成され、これが書き込み回路6 2 4 に出力される。

ステップS T 9 4 :

書き込み回路6 2 4 によって、復号回路6 2 3 から入力した個人情報D 1 が記録媒体6 1 5 に書き込まれる。

以上説明したように、情報復元装置6 3 1 によれば、正当な者が当該装置を用いることで、前述した第1 0 実施形態の情報記録装置6 0 1 によって別々の記録媒体6 1 6, 6 1 7 に格納されたモジュールD 3, D 4 から個人情報D 1 を復元できる。

第1 2 実施形態

図6 0 は、本実施形態の情報記録装置6 4 1 の構成図である。

図6 0 に示すように、情報記録装置6 4 1 は、読み出し回路6 5 0、情報分割回路6 5 1、暗号化回路6 5 2, 6 5 3 および書き込み回路6 5 4, 6 5 5 を有する。

本実施形態は、第3 0、3 2 および3 4 の発明に対応した実施形態である。

情報記録装置6 4 1 は、記録媒体6 1 5 から読み出した個人情報D 1 を、それぞれを単独では個人情報D 1 の秘匿性が保持される2つのモジュールD 1 2, D 1 3 に分割した後に暗号化してモジュールD 1 4, D 1 5 を生成し、モジュールD 1 4 を記録媒体6 1 6 に書き込み、モジュールD 1 5 を記録媒体6 1 7 に書き込む。

読み出し回路6 5 0 は、記録媒体6 1 5 から読み出した個人情報D 1 を情報分

割回路 6 5 1 に出力する。

個人情報 D 1 は、図 6 1 に示すように、情報 Data 1 ~ Data N からなる。また、個人情報 D 1 は、例えば、ユーザの個人 ID 情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

情報分割回路 6 5 1 は、読み出し回路 6 5 0 から入力した個人情報 D 1 を、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2, D 1 3 に分割し、モジュール D 1 2 を暗号化回路 6 5 2 に出力し、モジュール D 1 3 を暗号化回路 6 5 3 に出力する。

図 6 1 に示すように、情報分割回路 6 5 1 は、情報 D 1 内の情報 Data 1 ~ Data N を、それぞれ情報 Data 1 A および Data 1 B、情報 Data 2 A および Data 2 B、情報 Data 3 A および Data 3 B、...、情報 Data K A および Data K B、...、情報 Data N A および Data N B に分割する。

そして、情報分割回路 6 5 1 は、情報 Data 1 A, Data 2 A, Data 3 A, ..., Data K A, ..., Data N A からなるモジュール D 1 2 を暗号化回路 6 5 2 に出力する。

また、情報分割回路 6 5 1 は、情報 Data 1 B, Data 2 B, Data 3 B, ..., Data K B, ..., Data N B からなるモジュール D 1 3 を暗号化回路 6 5 3 に出力する。

暗号化回路 6 5 2 は、所定の暗号鍵を用いて、情報分割回路 6 5 1 から入力した個人情報 D 1 2 を暗号化して個人情報 D 1 4 を生成し、これを書き込み回路 6 5 4 に出力する。

暗号化された個人情報 D 1 4 は、図 6 1 に示すように、それぞれ情報 Data 1 A ~ Data N A を暗号化した情報 Data 1 A' ~ Data N A' からなる。

暗号化回路 6 5 3 は、所定の暗号鍵を用いて、情報分割回路 6 5 1 から入力した個人情報 D 1 3 を暗号化して個人情報 D 1 5 を生成し、これを書き込み回路 6 5 5 に出力する。暗号化回路 6 5 3 が用いる暗号鍵は、暗号化回路 6 5 2 が用いる暗号鍵と同じものを用いてもよいし、異なるものを用いてもよい。

暗号化された個人情報 D 1 5 は、図 6 1 に示すように、それぞれ情報 Data 1 B ~ Data NB を暗号化した情報 Data 1 B' ~ Data NB' からなる。

書き込み回路 6 5 4 は、暗号化回路 6 5 2 から入力したモジュール D 1 4 を記録媒体 6 1 6 に書き込む。

書き込み回路 6 5 5 は、暗号化回路 6 5 3 から入力したモジュール D 1 5 を記録媒体 6 1 7 に書き込む。

以下、情報記録装置 6 0 1 の動作を説明する。

図 6 2 は、情報記録装置 6 4 1 の動作を説明するためのフローチャートである。

ステップ S T 1 3 1 :

読み出し回路 6 5 0 によって、記録媒体 6 1 5 から図 6 1 に示す個人情報 D 1 が読み出されて情報分割回路 6 5 1 に出力される。

ステップ S T 1 3 2 :

情報分割回路 6 5 1 において、図 6 1 に示すように、読み出し回路 6 5 0 から入力した個人情報 D 1 が、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2, D 1 3 に分割され、モジュール D 1 2 が暗号化回路 6 5 2 に出力され、モジュール D 1 3 が暗号化回路 6 5 3 に出力される。

ステップ S T 1 3 3 :

暗号化回路 6 5 2 において、図 6 1 に示すように、所定の暗号鍵を用いて、情報分割回路 6 5 1 から入力した個人情報 D 1 2 が暗号化されて個人情報 D 1 4 が生成され、これを書き込み回路 6 5 4 に出力される。

また、暗号化回路 6 5 3 において、図 6 1 に示すように、所定の暗号鍵を用いて、情報分割回路 6 5 1 から入力した個人情報 D 1 3 が暗号化されて個人情報 D 1 5 が生成され、これが書き込み回路 6 5 5 に出力される。

ステップ S T 1 3 4 :

書き込み回路 6 5 4 によって、暗号化回路 6 5 2 から入力したモジュール D 1 4 が記録媒体 6 1 6 に書き込まれる。

書き込み回路 6 5 5 によって、暗号化回路 6 5 3 から入力したモジュール D 1 5 が記録媒体 6 1 7 に書き込まれる。

以上説明したように、情報記録装置 6 4 1 によれば、図 6 1 に示すように、個人情報 D 1 が、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2, D 1 3 に分割された後に暗号化されてモジュール D 1 4, D 1 5 が生成され、モジュール D 1 4, D 1 5 がそれぞれ物理的に独立した記録媒体 6 1 6, 6 1 7 にそれぞれ記録される。

そのため、記録媒体 6 1 6, 6 1 7 を別々に保管すれば、記録媒体 6 1 6, 6 1 7 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D 1 の秘匿性は保たれる。

。

第 1 3 実施形態

図 6 3 は、本実施形態の情報復元装置 6 6 1 の構成図である。

情報復元装置 6 6 1 は、上述した第 1 2 実施形態の情報記録装置 6 4 1 によって、記録媒体 6 1 6 と 6 1 7 とに分割して記録された個人情報から、本来の個人情報 D 1 を復元する。

図 6 3 に示すように、情報復元装置 6 6 1 は、読み出し回路 6 7 0, 6 7 1、復号回路 6 7 2, 6 7 3、情報合成回路 6 7 4 および書き込み回路 6 7 5 を有する。

本実施形態は、第 3 1 および第 3 3 の発明に対応した実施形態である。

図 6 3 において、記録媒体 6 1 6 および 6 1 7 には、前述した第 1 2 実施形態で説明した処理を経て、それぞれモジュール D 1 4 および D 1 5 が記録されている。

読み出し回路 6 7 0 は、記録媒体 6 1 6 から読み出したモジュール D 1 4 を復号回路 6 7 2 に出力する。

読み出し回路 6 7 1 は、記録媒体 6 1 7 から読み出したモジュール D 1 5 を復号回路 6 7 3 に出力する。

復号回路 6 7 2 は、読み出し回路 6 7 0 から入力したモジュール D 1 4 を、所定の復号鍵を用いて復号してモジュール D 1 2 を生成し、これを情報合成回路 6 7 4 に出力する。

復号回路 6 7 3 は、読み出し回路 6 7 1 から入力したモジュール D 1 5 を、所定の復号鍵を用いて復号してモジュール D 1 3 を生成し、これを情報合成回路 6 7 4 に出力する。

情報合成回路 6 7 4 は、図 6 4 に示すように、復号回路 6 7 2 から入力したモジュール D 1 2 と、復号回路 6 7 3 から入力したモジュール D 1 3 とを合成して個人情報 D 1 を生成し、これを書き込み回路 6 7 5 に出力する。

書き込み回路 6 7 5 は、情報合成回路 6 7 4 から入力した個人情報 D 1 を、記録媒体 6 1 5 に書き込む。

以下、情報復元装置 6 6 1 の動作を説明する。

図 6 5 は、情報復元装置 6 6 1 の動作を説明するためのフローチャートである。
。 ステップ S T 1 4 1 :

読み出し回路 6 7 0 によって、図 6 4 に示すように、記録媒体 6 1 6 からモジュール D 1 4 が読み出されて復号回路 6 7 2 に出力される。

また、読み出し回路 6 7 1 によって、記録媒体 6 1 7 からモジュール D 1 5 が読み出されて復号回路 6 7 3 に出力される。

ステップ S T 1 4 2 :

復号回路 672 において、読み出し回路 670 から入力したモジュール D14 が、所定の復号鍵を用いて復号されてモジュール D12 が生成され、これが情報合成回路 674 に出力される。

また、復号回路 673 において、読み出し回路 671 から入力したモジュール D15 が、所定の復号鍵を用いて復号されてモジュール D13 が生成され、これが情報合成回路 674 に出力される。

ステップ ST143 :

情報合成回路 674 において、図 64 に示すように、復号回路 672 から入力したモジュール D12 と、復号回路 673 から入力したモジュール D13 とが合成されて個人情報 D1 が生成され、これが書き込み回路 675 に出力される。

ステップ ST144 :

書き込み回路 675 によって、情報合成回路 674 から入力された個人情報 D1 が、記録媒体 615 に書き込まれる。

以上説明したように、情報復元装置 631 によれば、正当な者が当該装置を用いることで、前述した第 12 実施形態の情報記録装置 641 によって別々の記録媒体 616, 17 に格納されたモジュール D14, D15 から個人情報 D1 を復元できる。

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、個人情報を分割して得た複数のモジュールを異なる記録媒体に記録する場合を例示したが、当該複数のモジュールを同じ記録媒体の異なる領域に記録してもよい。この場合に、記録媒体の何れの領域に何れもモジュールを記録したかを秘密にしておけば、当該記録媒体を不正に取得した者は、記録媒体から読み出したモジュールの合成の仕方が分からず、個人情報を復元できない。

また、上述した実施形態では、所定の情報を分割する前後の何れか一方で暗号化を行う場合を例示したが、所定の情報を分割する前後の何れでも暗号化を行う

場合、並びに所定の情報を分割する前後の双方で暗号化を行う場合でも本発明は適用可能である。

また、上述した実施形態では、本発明の所定の情報として、個人情報を例示したが、その他、映像、音声などの情報であってもよい。

また、上述した実施形態では、個人情報を2分割して2つの記録媒体616, 617に記録する場合を例示したが、個人情報を3分割以上して3つ以上の記録媒体に記録してもよい。

産業上の利用可能性

以上説明したように本発明によれば、ネットワークを介した電子商取引の安全性を高めことができる認証装置、処理装置、認証システムおよびその方法を提供できる。

また、本発明によれば、第1の取引引き者の個人キー情報が第2の取引引き者に提供されないようにすることで、個人キー情報を用いた不正行為を効果的に抑制する認証装置、処理装置、認証システムおよびその方法を提供できる。

また、本発明によれば、不正に取得した他人の識別情報（個人ID情報）に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供できる。

また、本発明によれば、例えば異なる認証機関と契約した複数の取引引き者間での取引引きの認証を、取引引き者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供できる。

また、本発明によれば、不正に取得した他人の識別情報（個人ID情報）に基づいて不正な手続が行われることを回避する通信装置、通信システムおよびその方法を提供できる。

また、本発明によれば、不正に取得した他人の識別情報（個人ID情報）に基

づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、複数の通信装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法およびその装置と、そのような形態で情報が記録された記録媒体とを提供できる。

また、本発明によれば、上述したような情報記録方法およびその装置によって記録媒体に記録された情報を適切に復元できる情報復元方法およびその装置を提供できる。

また、本発明によれば、個人認証機能を持つ携帯型メモリ装置を用いて認証を行う場合に、煩雑な手続きを行うことなく、その安全性を高めることができる。

また、本発明によれば、第2の取り引き者が、取り引き識別情報を用いて、同じ取り引きについて第1の取り引き者の口座から複数回の引き落としが行われることを回避できる認証装置、認証システムおよびその方法を提供できる。

請求の範囲

1. ネットワークを介して少なくとも2者間で行われる取引を認証する認証装置において、

第1の取引者の個人キー情報および取引内容を示す情報を含む第1の要求を、前記第1の取引者から受信する第1の受信手段と、

前記第1の要求に含まれる前記個人キー情報に基づいて前記第1の取引者の正当性を認証して第1の認証情報を生成する第1の認証手段と、

前記第1の要求から前記第1の取引者の個人キー情報を除去した情報と、前記第1の認証情報とを含む第2の要求を第2の取引者に送信する第1の送信手段と、

前記第2の要求に対しての応答を前記第2の取引者から受信する第2の受信手段と、

前記応答に応じて、前記第2の取引者の正当性を認証して第2の認証情報を生成する第2の認証手段と、

前記第2の認証情報を前記第1の取引者に送信する第2の送信手段と

を有する認証装置。

2. 前記第1の取引者の個人キー情報は前記第1の取引者の課金に係わる情報である

請求項1に記載の認証装置。

3. 前記取引の履歴を示す履歴情報を記憶する記憶手段

をさらに有する請求項1に記載の認証装置。

4. ネットワークを介して少なくとも2者間で行われる取引を認証する認証システムにおいて、

第1の取引者が使用する第1の通信装置と、

第 2 の取り引き者が使用する第 2 の通信装置と、
前記取り引きを認証する認証装置と

を有し、

前記認証装置は、

第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む
第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、

前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り
引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情
報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信す
る第 1 の送信手段と、

前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第
2 の受信手段と、

前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認
証情報を生成する第 2 の認証手段と、

前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段
と

を有する

認証システム。

5. ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する
認証方法において、

第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む
第 1 の要求を、前記第 1 の取り引き者から受信し、

前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り
引き者の正当性を認証して第 1 の認証情報を生成し、

前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情

報と、前記第 1 の認証情報とを含む第 2 の要求を第 2 の取引引き者に送信し、

前記第 2 の要求に対しての応答を前記第 2 の取引引き者から受信し、

前記応答に応じて、前記第 2 の取引引き者の正当性を認証して第 2 の認証情報を生成し、

前記第 2 の認証情報を前記第 1 の取引引き者に送信する

認証方法。

6. 前記第 1 の取引引き者の個人キー情報を用いて、前記取引引きの決済を行う

請求項 5 に記載の認証方法。

7. ネットワークを介して少なくとも 2 者間で行われる取引引きを認証する認証装置において、

第 1 の取引引き者の個人識別情報および取引引き内容を示す情報を含む第 1 の要求を、前記第 1 の取引引き者から受信する第 1 の受信手段と、

前記第 1 の要求に応じて、前記第 1 の取引引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の認証情報および前記取引引きの内容を示す情報を含む第 2 の要求を第 2 の取引引き者に送信する第 1 の送信手段と、

前記第 2 の要求に対しての応答を前記第 2 の取引引き者から受信する第 2 の受信手段と、

前記応答に応じて、前記第 2 の取引引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、

前記第 2 の認証情報を前記第 1 の取引引き者に送信する第 2 の送信手段と

を有する認証装置。

8. 前記第 1 の受信手段は、前記第 1 の取引引き者の個人キー情報をさらに含む前記第 1 の要求を受信し、

前記第 1 の認証手段は、前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証する

請求項 7 に記載の認証装置。

9. 前記第 1 の取り引き者の前記個人キー情報は、前記第 1 の取り引き者の課金に係わる情報である

請求項 8 に記載の認証装置。

10. 前記第 1 の送信手段は、前記第 1 の取り引き者の前記個人キー情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する

請求項 9 に記載の認証装置。

11. 前記取り引きの履歴を示す履歴情報を記憶する記憶手段

をさらに有する請求項 7 に記載の認証装置。

12. 前記第 1 の要求が暗号化されている場合に、前記受信した第 1 の要求を復号する復号手段

をさらに有する請求項 7 に記載の認証装置。

13. 前記第 2 の要求を暗号化する暗号化手段

をさらに有する請求項 7 に記載の認証装置。

14. 前記応答が暗号化されている場合に、前記受信した応答を復号する復号手段

をさらに有する請求項 7 に記載の認証装置。

15. 前記第 2 の認証情報を暗号化する暗号化手段

をさらに有する請求項 7 に記載の認証装置。

16. ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムにおいて、

第 1 の取り引き者が使用する第 1 の通信装置と、

第 2 の取り引き者が使用する第 2 の通信装置と、

前記取り引きを認証する認証装置と

を有し、

前記第 1 の通信装置は、第 1 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を前記認証装置に送信し、

前記認証装置は、

前記第 1 の取り引き者から前記第 1 の要求を受信する第 1 の受信手段と

、
前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、

前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、

前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、

前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段と

を有する

認証システム。

17. 前記第 1 の受信手段は、前記第 1 の取り引き者の個人キー情報をさらに含む前記第 1 の要求を受信し、

前記第 1 の認証手段は、前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証する

請求項 16 に記載の認証システム。

18. 前記第 1 の取り引き者の前記個人キー情報は、前記第 1 の取り引き者の課金に係わる情報である

請求項 17 に記載の認証システム。

19. ネットワークを介して少なくとも2者間で行われる取引きを認証する認証方法において、

第1の取引き者の個人識別情報および取引き内容を示す情報を含む第1の要求を、前記第1の取引き者から受信し、

前記第1の要求に応じて、前記第1の取引き者の正当性を認証して第1の認証情報を生成し、

前記第1の認証情報および前記取引きの内容を示す情報を含む第2の要求を前記第2の取引き者に送信し、

前記第2の要求に対しての応答を前記第2の取引き者から受信し、

前記応答に応じて、前記第2の取引き者の正当性を認証して第2の認証情報を生成し、

前記第2の認証情報を前記第1の取引き者に送信する

認証方法。

20. 前記第1の取引き者の個人キー情報をさらに含む前記第1の要求を受信し、

前記個人キー情報に基づいて前記第1の取引き者の正当性を認証する

請求項19に記載の認証方法。

21. 前記第1の取引き者の前記個人キー情報は、前記第1の取引き者の課金に係わる情報である

請求項20に記載の認証方法。

22. 前記第1の取引き者の前記個人キー情報をさらに含む第2の要求を前記第2の取引き者に送信する

請求項21に記載の認証方法。

23. 前記第2の取引き者は、前記第1の取引き者の個人キー情報を用いて決済を行う

請求項 2 2 に記載の認証方法。

2 4. 第 1 の取り引き者に関する情報を保持し、第 2 の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果を示す第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける送受信手段と、

前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、

前記所定の応答を受けた場合に、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される第 2 の署名情報であって、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成する署名作成手段と

を有する認証装置。

2 5. 暗号化手段

をさらに有し、

前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する

請求項 2 4 に記載の認証装置。

26. 前記送受信手段は、

前記他の認証装置が前記第2の取引引き者を識別するために用いる識別情報を含む前記所定の応答を前記第2の取引引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取引引きの履歴を記憶する

請求項24に記載の認証装置。

27. 前記送受信手段は、前記第1の要求に含まれる前記取引引き内容に関する情報のうち、前記第1の取引引き者の課金に係わる情報以外の情報と、前記第1の署名情報とを含む第3の要求を前記第2の取引引き者が使用する装置に送信する

請求項24に記載の認証装置。

28. 前記送受信手段は、前記第1の要求に含まれる前記取引引き内容に関する情報と、前記第1の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第3の要求を前記第2の取引引き者が使用する装置に送信する

請求項24に記載の認証装置。

29. 前記取引引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する請求項24に記載の認証装置。

30. 前記課金処理手段は、前記他の認証装置との間で、前記取引引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項24に記載の認証装置。

31. 前記送受信手段は、前記第2の取引引き者が前記第1の署名情報の正当性を確認して、当該取引引きに同意した場合に、前記第2の取引引き者が使用する装置から、前記所定の応答を受ける

請求項24に記載の認証装置。

32. 前記送受信手段は、

前記第2の署名情報を前記第2の取引引き者が使用する装置に送信する

請求項 2 4 に記載の認証装置。

3 3. ネットワークを介して少なくとも 2 者間で行われた取引引きを認証する認証システムにおいて、

第 1 の取引引き者に関する取引引きを認証する第 1 の認証装置と、
第 2 の取引引き者に関する取引引きを認証する第 2 の認証装置と
を有し、

前記第 1 の認証装置は、

前記取引引き内容を示す情報と前記第 2 の取引引き者を特定する情報とを含む前記第 1 の取引引き者による第 1 の要求に応じて、前記第 2 の取引引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果である第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取引引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取引引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取引引き者から所定の応答を受けると、前記取引引きの履歴を記憶し、前記取引引きの正当性の認証結果を示す第 2 の署名情報を前記第 1 の取引引き者に提供する

認証システム。

3 4. 前記第 1 の認証装置は、

暗号化手段

をさらに有し、

前記送受信手段は、前記第 2 の取引引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記第 2 の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取引引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取引引き者が使用する装置に送信する

請求項 3 3 に記載の認証システム。

35. 前記第1の認証装置の前記送受信手段は、

前記第2の認証装置が前記第2の取引引き者を識別するために用いる識別情報を含む前記所定の応答を前記第2の取引引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取引引きの履歴を記憶する

請求項33に記載の認証システム。

36. 前記第1の認証装置は、

前記第2の署名情報を前記第2の取引引き者に提供する

請求項33に記載の認証システム。

37. 第1の取引引き者に関する取引引きを認証する第1の認証装置と、第2の取引引き者に関する取引引きを認証する第2の認証装置とを用いて、ネットワークを介して行われる前記第1の取引引き者と前記第2の取引引き者との間の取引引きに関する認証を行う認証方法であって、

前記第1の取引引き者から前記第1の認証装置に、前記取引引き内容を示す情報と前記第2の取引引き者を特定する情報とを含む第1の要求を出し、

前記第1の要求に応じて、前記第1の認証装置から前記第2の認証装置に、前記第2の取引引き者を特定する情報を含む第2の要求を送信し、

前記第2の要求に応じて、前記第2の認証装置からの前記第1の認証装置に、当該第2の認証装置による認証結果を示す第1の署名情報を送信し、

前記第1の認証装置から前記第2の取引引き者が使用する装置に、前記第1の要求に含まれる前記取引引き内容に関する情報と前記第1の署名情報とを含む第3の要求を送信し、

当該第3の要求に応じて、前記第2の取引引き者が使用する装置から前記第1の認証装置に所定の応答を出し、

前記所定の応答に応じて、前記第1の認証装置は、前記取引引きの履歴

を記憶し、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成し、当該第 2 の署名情報を、前記第 1 の取り引き者が使用する装置に送信する

認証方法。

38. 前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて、前記第 2 の認証装置から前記第 1 の認証装置に送信し、

前記第 1 の認証装置は、前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第 2 の取り引き者が使用する装置に送信する

請求項 37 に記載の認証方法。

39. 前記第 1 の認証装置は、前記第 2 の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項 37 に記載の認証方法。

40. 前記第 1 の要求に含まれる前記取り引き内容に関する情報のうち、前記第 1 の取り引き者の課金に係わる情報以外の情報と、前記第 1 の署名情報とを含む第 3 の要求を、前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に送信する

請求項 37 に記載の認証方法。

41. 前記第 1 の要求に含まれる前記取り引き内容に関する情報と、前記第 1 の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第 3 の要求を、前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に送信する

請求項 37 に記載の認証方法。

42. 前記第 1 の認証装置と前記第 2 の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項 37 に記載の認証方法。

4 3. 前記第 2 の取り引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から前記第 1 の認証装置に、前記所定の応答を出す

請求項 3 7 に記載の認証方法。

4 4. 前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に、前記第 2 の署名情報を送信する

請求項 3 7 に記載の認証方法。

4 5. 第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証方法であって、

前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 1 の取り引き者の個人キー情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、

前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 1 の要求から前記個人キーを除去した第 2 の要求を送信し、

前記第 2 の要求に応じて、前記取り引きの内容を示す情報を含む第 3 の要求を、前記第 2 の認証装置から前記第 2 の取り引き者が使用する装置に送信し、

前記第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から前記第 2 の認証装置に第 1 の応答を送信し、

前記第 1 の応答に応じて、前記第 2 の認証装置から前記第 1 の認証装置に、前記第 2 の取り引き者への支払い方法を示す支払い方法情報を含む第 2 の応答を送信し、

前記第 1 の認証装置は、前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取り引き者との間の前記取り引き者に関する支払いを管理

する

認証方法。

46. 前記第1の認証装置は、前記取り引きに関して、前記第1の取り引き者から支払い金を受けるための処理と、前記支払い金の一部を前記取り引きに応じて前記第2の取り引き者に支払う処理と、前記支払い金の残りを手数料として受け取る処理と行う

請求項45に記載の認証方法。

47. 前記第1の認証装置は、前記第1の要求に応じて、前記第2の取り引き者が前記第2の認証装置と契約しているか否かを前記第2の認証装置に問い合わせ、契約している旨の回答を前記第2の認証装置から受信した場合に、前記第2の要求を前記第2の認証装置に送信する

請求項45に記載の認証方法。

48. 前記第1の認証装置は、前記第2の応答を受信すると、前記取り引き者について当該第1の認証装置が行った認証結果を含む署名情報を含む第3の応答を、前記第1の取り引き者が使用する装置に送信する

請求項45に記載の認証方法。

49. 前記第1の認証装置は、当該第1の認証装置に対応する秘密鍵を用いて、前記第3の応答を暗号化して前記第1の取り引き者が使用する装置に送信する

請求項48に記載の認証方法。

50. 前記第1の認証装置は、前記取り引きについて当該第1の認証装置が行った認証結果を示す署名情報をさらに含む前記第2の要求を前記第2の認証装置に送信する

請求項45に記載の認証方法。

51. 前記第2の認証装置は、前記取り引きについて当該第2の認証装置が行った認証結果を示す署名情報をさらに含む前記第3の要求を前記第2の取り引き

者が使用する装置に送信する

請求項 4 5 に記載の認証方法。

5 2. 前記第 1 の認証装置は、当該第 1 に認証装置に対応する秘密鍵を用いて、前記第 2 の要求を暗号化して前記第 2 の認証装置に送信する

請求項 4 5 に記載の認証方法。

5 3. 前記第 2 の認証装置は、当該第 2 の認証装置に対応する秘密鍵を用いて、前記第 3 の要求を暗号化して前記第 2 の取り引き者が使用する装置に送信する

請求項 4 5 に記載の認証方法。

5 4. 前記第 2 の取り引き者の装置は、当該第 2 の取り引き者の秘密鍵を用いて、前記第 1 の応答を暗号化して前記第 2 の認証装置に送信する

請求項 4 5 に記載の認証方法。

5 5. 前記第 2 の認証装置は、当該第 2 に認証装置に対応する秘密鍵を用いて、前記第 2 の応答を暗号化して前記第 1 の認証装置に送信する

請求項 4 5 に記載の認証方法。

5 6. 第 1 の取り引き者に関する情報を保持し、第 2 の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第 1 の取り引き者の個人キー情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を前記第 1 の取り引き者から受信し、前記第 2 の取り引き者への支払い方法を示す支払い方法情報を含む応答を前記他の認証装置から受信する受信手段と、

前記第 1 の要求に応じて、前記第 1 の要求から前記個人キーを除去した第 2 の要求を前記他の通信装置に送信する送信手段と、

前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取

り引き者との間の前記取り引き者に関する支払いを管理する課金手段と
を有する認証装置。

57. 前記課金手段は、前記取り引きに関して、前記第1の取り引き者から支払い金を受けるための処理と、前記支払い金の一部を前記取り引きに応じて前記第2の取り引き者に支払う処理と、前記支払い金の残りを手数料として受け取る処理と行う

請求項56に記載の認証装置。

58. 前記送信手段は、前記第1の要求に応じて、前記第2の取り引き者が前記第2の認証装置と契約しているか否かを前記他の認証装置に問い合わせ、契約している旨の回答を前記受信手段が前記他の認証装置から受信した場合に、前記第2の要求を前記他の認証装置に送信する

請求項56に記載の認証装置。

59. 前記送信手段は、前記第2の応答を前記受信手段が受信すると、前記取り引き者について自らが行った認証結果を含む署名情報を含む応答を、前記第1の取り引き者が使用する装置に送信する

請求項56に記載の認証装置。

60. 前記送信手段は、当該第1の認証装置に対応する秘密鍵を用いて、前記応答を暗号化して前記第1の取り引き者が使用する装置に送信する

請求項59に記載の認証装置。

61. 前記送信手段は、前記取り引きについて当該第1の認証装置が行った認証結果を示す署名情報をさらに含む前記第2の要求を前記他の認証装置に送信する

請求項56に記載の認証装置。

62. 第1の取り引き者に関する取り引きを認証する第1の認証装置と、第2の取り引き者に関する取り引きを認証する第2の認証装置とを有し、ネットワークを介して行われる前記第1の取り引き者と前記第2の取り引き者との間の取り

引きに関する認証を行う認証システムであって、

前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 1 の取り引き者の個人キー情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、

前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 1 の要求から前記個人キーを除去した第 2 の要求を送信し、

前記第 2 の要求に応じて、前記取り引きの内容を示す情報を含む第 3 の要求を、前記第 2 の認証装置から前記第 2 の取り引き者が使用する装置に送信し、

前記第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から前記第 2 の認証装置に第 1 の応答を送信し、

前記第 1 の応答に応じて、前記第 2 の認証装置から前記第 1 の認証装置に、前記第 2 の取り引き者への支払い方法を示す支払い方法情報を含む第 2 の応答を送信し、

前記第 1 の認証装置は、前記支払い方法情報に基づいて、前記第 1 の取り引き者と前記第 2 の取り引き者との間の前記取り引き者に関する支払いを管理する

認証システム。

6 3. 前記第 1 の認証装置は、前記取り引きに関して、前記第 1 の取り引き者から支払い金を受けるための処理と、前記支払い金の一部を前記取り引きに応じて前記第 2 の取り引き者に支払う処理と、前記支払い金の残りを手数料として受け取る処理と行う

請求項 6 2 に記載の認証システム。

6 4. 前記第 1 の認証装置は、前記第 1 の要求に応じて、前記第 2 の取り引き者が前記第 2 の認証装置と契約しているか否かを前記第 2 の認証装置に問い合わせ、契約している旨の回答を前記第 2 の認証装置から受信した場合に、前記第 2

の要求を前記第 2 の認証装置に送信する

請求項 6 2 に記載の認証システム。

6 5. 前記第 1 の認証装置は、前記第 2 の応答を受信すると、前記取り引き者について当該第 1 の認証装置が行った認証結果を含む署名情報を含む第 3 の応答を、前記第 1 の取り引き者が使用する装置に送信する

請求項 6 2 に記載の認証システム。

6 6. 前記第 1 の認証装置は、当該第 1 の認証装置に対応する秘密鍵を用いて、前記第 3 の応答を暗号化して前記第 1 の取り引き者が使用する装置に送信する

請求項 6 5 に記載の認証システム。

6 7. 前記第 1 の認証装置は、前記取り引きについて当該第 1 の認証装置が行った認証結果を示す署名情報をさらに含む前記第 2 の要求を前記第 2 の認証装置に送信する

請求項 6 2 に記載の認証システム。

6 8. 前記第 2 の認証装置は、前記取り引きについて当該第 2 の認証装置が行った認証結果を示す署名情報をさらに含む前記第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する

請求項 6 2 に記載の認証システム。

6 9. 前記第 1 の認証装置は、当該第 1 に認証装置に対応する秘密鍵を用いて、前記第 2 の要求を暗号化して前記第 2 の認証装置に送信する

請求項 6 2 に記載の認証システム。

7 0. 前記第 2 の認証装置は、当該第 2 の認証装置に対応する秘密鍵を用いて、前記第 3 の要求を暗号化して前記第 2 の取り引き者が使用する装置に送信する

請求項 6 2 に記載の認証システム。

7 1. 前記第 2 の取り引き者の装置は、当該第 2 の取り引き者の秘密鍵を用い

て、前記第 1 の応答を暗号化して前記第 2 の認証装置に送信する

請求項 6 2 に記載の認証システム。

7 2. 前記第 2 の認証装置は、当該第 2 に認証装置に対応する秘密鍵を用いて、前記第 2 の応答を暗号化して前記第 1 の認証装置に送信する

請求項 6 2 に記載の認証システム。

7 3. 認証装置において、ユーザの認証情報を第 1 の認証情報および第 2 の認証情報に分割し、

前記第 2 の認証情報を記憶した携帯型メモリ装置を前記ユーザに提供し、

前記携帯型メモリ装置にアクセス可能な端末装置から前記認証装置に認証情報要求を送信し、

前記認証装置において、前記認証情報要求が正当なユーザによるものであると判断した場合に、前記認証装置から前記端末装置に前記第 1 の認証情報を送信し、

前記端末装置において、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とを用いて前記認証情報を復元する

認証方法。

7 4. 前記認証情報要求は、前記第 1 の認証情報の送信先を指定した送信先情報を含み、

前記認証装置は、前記送信先情報で指定された前記端末装置に、前記第 1 の認証情報を送信する

請求項 7 3 に記載の認証方法。

7 5. 前記認証装置は、前記ユーザに対応する送信先情報を予め記憶し、当該記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項 7 4 に記載の認証方法。

7 6. 前記端末装置は、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とが対応していると判断した場合に、前記受信した第 1 の認証情報を記憶して前記認証情報を復元する

請求項 7 3 に記載の認証方法。

7 7. 前記端末装置は、前記認証装置から受信した前記第 1 の認証情報と、前記携帯型メモリ装置から読み出した前記第 2 の認証情報とが対応していない場合に、その旨を示す通知を前記認証装置に送信する

請求項 7 3 に記載の認証方法。

7 8. 前記認証装置は、前記ユーザからの要求に応じて、前記認証情報を生成する

請求項 7 3 に記載の認証方法。

7 9. 前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項 7 3 に記載の認証方法。

8 0. 前記携帯型メモリ装置は、スマートカードである

請求項 7 3 に記載の認証方法。

8 1. 認証情報を生成し、

前記認証情報を第 1 の認証情報および第 2 に認証情報に分割し、

前記第 2 の認証情報を記憶した携帯型メモリ装置をユーザに提供し、

受信した認証情報要求が正当なユーザによるものであると判断した場合に、前記認証情報要求が指定する送信先に、前記第 1 の認証情報を送信する

認証方法。

8 2. 前記ユーザに対応する送信先情報を予め記憶し、

前記記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項 8 1 に記載の認証方法。

8 3. 前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項 8 1 に記載の認証方法。

8 4. 前記携帯型メモリ装置は、スマートカードである

請求項 8 1 に記載の認証方法。

8 5. 認証情報を生成し、前記認証情報を第 1 の認証情報および第 2 に認証情報に分割し、受信した認証情報要求が正当なユーザによるものであるか否かを判断する制御手段と、

携帯型メモリ装置に前記第 2 の認証情報を書き込む書込手段と、

前記携帯型メモリ装置のユーザから前記認証情報要求を受信する受信手段と、

前記認証情報要求が正当なユーザによるものであると判断された場合に、前記第 1 の認証情報を前記認証情報要求によって指定された送信先に送信する送信手段と

を有する認証装置。

8 6. 前記ユーザに対応する送信先情報を予め記憶する記憶手段

をさらに有し、

前記制御手段は、前記記憶した送信先情報に、前記認証情報要求によって指定された送信先が示されている場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項 8 5 に記載の認証装置。

8 7. 前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項 8 5 に記載の認証装置。

8 8. 前記携帯型メモリ装置は、スマートカードである

請求項 8 5 に記載の認証装置。

8 9. 利用者を識別するための個人識別情報を含む要求を受信する受信手段と

前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段と

を有する通信装置。

90. 前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段をさらに有する請求項89に記載の通信装置。

91. 前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である

請求項89に記載の通信装置。

92. 前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である

請求項89に記載の通信装置。

93. 前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項89に記載の通信装置。

94. 前記処理は、認証処理である

請求項89に記載の通信装置。

95. ネットワークを介して接続される第1の通信装置および第2の通信装置

を有する通信システムであって、

前記第 1 の通信装置は、

利用者を識別するための個人識別情報を含む要求を受信する第 1 の受信手段と、

前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第 1 の送信手段と

を有し、

前記第 2 の通信装置は、

前記要求を前記第 1 の通信装置に送信する第 2 の送信手段と、

前記処理の結果を前記第 1 の通信装置から受信する第 2 の受信手段と、

当該受信した認証処理の結果を出力する出力手段と

を有する

通信システム。

9 6. 前記第 1 の通信装置の前記第 1 の受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記第 1 の通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段

をさらに有する請求項 9 5 に記載の通信システム。

9 7. 前記個人識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられた識別子である

請求項 9 5 に記載の通信システム。

9 8. 前記処理の結果を送信する送信先の情報は、前記第 2 の通信装置の利用者がオフラインで当該第 1 の通信装置に提供した情報である

請求項 9 5 に記載の通信システム。

9 9. 前記処理の結果を送信する送信先の情報は、前記第 1 の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項 9 5 に記載の通信システム。

1 0 0. ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を用いた通信方法であって、

利用者を識別するための個人識別情報を含む要求を、前記第 2 の通信装置から前記第 1 の通信装置に送信し、

前記第 1 の通信装置において、前記要求に応じて所定の処理を行い、

前記第 1 の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する

通信方法。

1 0 1. 前記第 2 の通信装置において前記第 1 の通信装置から受信した前記処理の結果を出力する

請求項 1 0 0 に記載の通信方法。

1 0 2. 前記第 1 の通信装置は、暗号化された前記個人識別情報を含む前記要求を受信し、当該受信した要求に含まれる前記個人識別情報を復号する

請求項 1 0 0 に記載の通信方法。

1 0 3. 前記個人識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられた識別子である

請求項 1 0 0 に記載の通信方法。

104. 前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該第1の通信装置に提供した情報である

請求項100に記載の通信方法。

105. 前記処理の結果を送信する送信先の情報は、前記第1の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項100に記載の通信方法。

106. ネットワークを介して少なくとも2者間で行われる取引を認証する認証装置において、

第1の取引者の個人キー情報および取引内容を示す情報を含む第1の要求を、前記第1の取引者から受信する第1の受信手段と、

前記第1の要求に含まれる前記個人キー情報に基づいて前記第1の取引者の正当性を認証して第1の認証情報を生成する第1の認証手段と、

前記第1の要求から前記第1の取引者の個人キー情報を除去した情報と、前記第1の認証情報とを含む第2の要求を前記第2の取引者に送信する第1の送信手段と、

前記第2の要求に対しての応答を前記第2の取引者から受信する第2の受信手段と、

前記応答に応じて、前記第2の取引者の正当性を認証して第2の認証情報を生成する第2の認証手段と、

前記第2の認証情報を前記第1の取引者に送信する第2の送信手段と、

前記第1の要求を受信したときに、取引識別情報を発行する取引識別情報発行手段と、

前記取引識別情報を用いて、前記第1の要求の受信、前記第2の要求の送信、並びに前記応答の受信の履歴を管理する取引履歴管理手段と

を有する認証装置。

107. 前記取り引き履歴管理手段は、

前記第1の要求の受信、前記第2の要求の送信、並びに前記応答の受信のそれぞれについて履歴情報を生成し、当該履歴情報を前記取り引き識別情報に関連付けて記憶する

請求項106に記載の認証装置。

108. 前記送信手段は、前記取り引き識別情報をさらに含む第2の要求を前記第2の取り引き者に送信する

請求項106に記載の認証装置。

109. 前記第2の認証手段は、前記応答に含まれる前記取り引き識別情報と、前記取り引き履歴管理手段が管理する前記履歴とに基づいて、前記応答の正当性を認証する

請求項108に記載の認証装置。

110. 前記取り引きに係わる決済処理を行う決済処理手段をさらに有し、

前記取り引き履歴管理手段は、

前記決済処理の終了後に、決済処理が終了したことを示す履歴情報を前記取り引き識別情報に関連付けて記憶する

請求項106に記載の認証装置。

111. 前記第1の取り引き者の個人キー情報は前記第1の取り引き者の課金に係わる情報である

請求項106に記載の認証装置。

112. ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証システムにおいて、

第1の取り引き者が使用する第1の通信装置と、

第2の取り引き者が使用する第2の通信装置と、

前記取り引きを認証する認証装置と

を有し、

前記認証装置は、

前記第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、

前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む前記第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、

前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、

前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、

前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段と、

前記第 1 の要求を受信したときに、取り引き識別情報を発行する取り引き識別情報発行手段と、

前記取り引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴を管理する取り引き履歴管理手段と

を有する

認証システム。

1 1 3. ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証方法において、

第 1 の取り引き者の個人キー情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信し、当該受信に応じて取り引き識

別情報を発行し、

前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取引引き者の正当性を認証して第 1 の認証情報を生成し、

前記第 1 の要求から前記第 1 の取引引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取引引き者に送信し

、
前記第 2 の要求に対しての応答を前記第 2 の取引引き者から受信し、

前記応答に応じて、前記第 2 の取引引き者の正当性を認証して第 2 の認証情報を生成し、

前記第 2 の認証情報を前記第 1 の取引引き者に送信し、

前記取引引き識別情報を用いて、前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信の履歴を管理する

認証方法。

1 1 4. 前記第 1 の要求の受信、前記第 2 の要求の送信、並びに前記応答の受信のそれぞれについて履歴情報を生成し、当該履歴情報を前記取引引き識別情報に関連付けて記憶する

請求項 1 1 3 に記載の認証方法。

1 1 5. 前記取引引き識別情報をさらに含む第 2 の要求を前記第 2 の取引引き者に送信する

請求項 1 1 4 に記載の認証方法。

1 1 6. 前記応答に含まれる前記取引引き識別情報と、前記取引引き履歴管理手段が管理する前記履歴とに基づいて、前記応答の正当性を認証する

請求項 1 1 4 に記載の認証方法。

1 1 7. 前記取引引きに係わる決済処理をさらにに行い、

前記決済処理の終了後に、決済処理が終了したことを示す履歴情報を前記取引引き識別情報に関連付けて記憶する

請求項 1 1 4 に記載の認証方法。

1 1 8. 前記第 2 の取り引き者の個人キー情報を含む前記応答を受信し、
前記第 2 の取り引き者の個人キー情報に基づいて前記第 2 の取り引き者の正当性を認証する

請求項 1 1 4 記載の認証方法。

1 1 9. 前記第 1 の取り引き者の個人キー情報は前記第 1 の取り引き者の課金に係わる情報であり、前記第 2 の取り引き者の個人キー情報は前記第 2 の取り引き者の課金に係わる情報である

請求項 1 1 8 に記載の認証方法。

1 2 0. 単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、

前記第 1 の通信装置を識別するための装置識別情報を記憶する記憶手段と、

前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を前記第 2 の通信装置に送信する送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する受信手段と、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と

を有する通信制御装置。

1 2 1. 前記制御手段は、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う

請求項 1 2 0 に記載の通信制御装置。

1 2 2. 前記制御手段は、

前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 2 0 に記載の通信制御装置。

1 2 3. 前記送信手段は、

前記第 1 の通信装置から受信した個人識別情報と、当該第 1 の通信装置に対応する前記装置識別情報とを含む前記要求を前記第 2 の通信装置に送信する

請求項 1 2 0 に記載の通信制御装置。

1 2 4. 前記記憶手段は、

前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 1 2 0 に記載の通信制御装置。

1 2 5. 前記記憶手段は、

当該通信制御装置の電源が投入されたときに前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 1 2 4 に記載の通信制御装置。

1 2 6. 前記制御手段は、

前記第 1 の通信装置と前記第 2 の通信装置との間の通信履歴を前記記憶手段に書き込む

請求項 1 2 0 に記載の通信制御装置。

1 2 7. 前記制御手段は、

前記応答に含まれる前記第 2 の通信装置の処理結果を、前記要求の送信元の前記第 1 の通信装置に送信する

請求項 1 2 0 に記載の通信制御装置。

1 2 8. 前記制御手段は、

前記受信手段から受信した情報に応じて、待機状態にある前記第 1 の通信装置が動作状態になるように制御する

請求項 1 2 0 に記載の通信制御装置。

1 2 9. 前記制御手段は、

前記第 1 の通信装置が接続されたネットワークと、前記第 2 の通信装置が接続されたネットワークとの間の通信を制御する

請求項 1 2 0 に記載の通信制御装置。

1 3 0. 前記制御手段は、

ゲートウェイとしての処理を行う

請求項 1 2 0 に記載の通信制御装置。

1 3 1. 前記装置識別情報は、前記第 1 の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である

請求項 1 2 0 に記載の通信制御装置。

1 3 2. 前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項 1 2 0 に記載の通信制御装置。

1 3 3. 前記受信手段は、

前記第 2 の通信装置が行った認証処理の結果を含む前記応答を前記第 2 の通信装置から受信する

請求項 1 2 0 に記載の通信制御装置。

1 3 4. 単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、

前記通信制御装置は、

前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記

憶手段と、

前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、

前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と

を有し、

前記第 2 の通信装置は、

前記要求を受信する第 2 の受信手段と、

前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段と

を有する

通信システム。

135. 単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、

前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当

該第 1 の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、

前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、

前記第 2 の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、

前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する

通信方法。

136. 前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う

請求項 135 に記載の通信方法。

137. 前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 135 に記載の通信方法。

138. 認証要求に応じて認証処理を行う認証装置であって、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記

憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

139. 前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項138に記載の認証装置。

140. 前記受信手段は、前記利用者に関する課金処理に用いられる第3の識別情報をさらに含む前記認証要求を受信する

請求項138に記載の認証装置。

141. 前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項138に記載の認証装置。

142. 前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である

請求項138に記載の認証装置。

143. ネットワークを介して行われる取引に関する認証処理を行う認証装置であって、

利用者を識別するための個人識別情報と、取引の内容を示す取引情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取

り引きを行う利用者による前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

1 4 4. 前記認証処理手段は、

前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する

請求項 1 4 3 に記載の認証装置。

1 4 5. 前記記憶手段は、

前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する

請求項 1 4 3 に記載の認証装置。

1 4 6. 前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項 1 4 3 に記載の認証装置。

1 4 7. 前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する

請求項 1 4 3 に記載の認証装置。

1 4 8. 前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する請求項 1 4 3 に記載の認証装置。

1 4 9. ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、

認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、

前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段と

を有する処理装置。

1 5 0. 前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 1 4 9 に記載の処理装置。

1 5 1. 前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 4 9 に記載の処理装置。

1 5 2. ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、

前記認証装置は、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段と

を有し、

前記処理装置は、

前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、

前記認証応答を受信する受信手段と、

当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段と

を有する

認証システム。

1 5 3. 前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 1 5 2 に記載の認証システム。

1 5 4. 前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 5 2 に記載の認証システム。

1 5 5. ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するため

の装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、

前記認証装置において前記認証要求に応じて認証処理を行い、

前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、

前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する

認証方法。

156. 前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する

請求項155に記載の認証方法。

157. 前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項155に記載の認証方法。

158. れ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

情報記録方法。

159. 前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項158に記載の情報記録方法。

160. 前記所定の情報を暗号化し、

当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性

が保持される前記複数のモジュールに分割する

請求項 1 5 8 に記載の情報記録方法。

1 6 1. 前記複数のモジュールをそれぞれ暗号化し、

当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

請求項 1 5 8 に記載の情報記録方法。

1 6 2. れ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、

当該読み出したモジュールを合成して前記所定の情報を復元する
情報復元方法。

1 6 3. 前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 6 2 に記載の情報復元方法。

1 6 4. 前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する

請求項 1 6 2 に記載の情報復元方法。

1 6 5. 前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する

請求項 1 6 2 に記載の情報復元方法。

1 6 6. それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段と

を有する情報記録装置。

1 6 7. 前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 6 6 に記載の情報記録装置。

1 6 8. 前記所定の情報を暗号化する暗号化手段

をさらに有し、

前記情報分割手段は、

前記暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項 1 6 6 に記載の情報記録装置。

1 6 9. 前記複数のモジュールをそれぞれ暗号化する暗号化手段

をさらに有し、

前記書き込み手段は、

前記暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む

請求項 1 6 6 に記載の情報記録装置。

1 7 0. それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と、

当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段と

を有する情報復元装置。

1 7 1. 前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 7 0 に記載の情報復元装置。

1 7 2. 前記合成して得た情報を復号する復号手段

をさらに有する

請求項 1 7 0 に記載の情報復元装置。

1 7 3. 前記読み出したモジュールを復号する復号手段

をさらに有し、

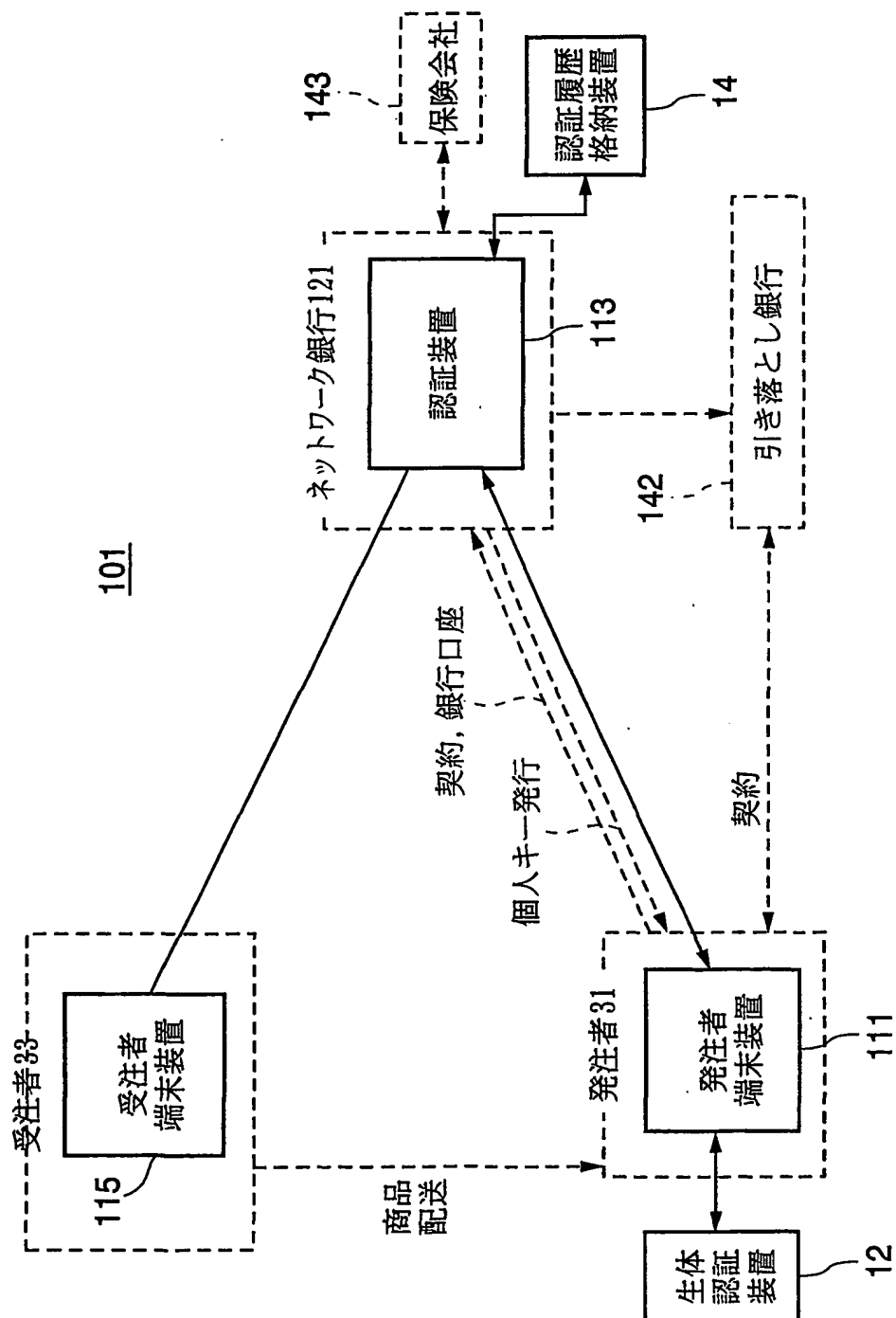
前記情報合成手段は、前記復号したモジュールを合成して前記所定の情報を復元する

請求項 1 7 0 に記載の情報復元装置。

1 7 4. それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録された

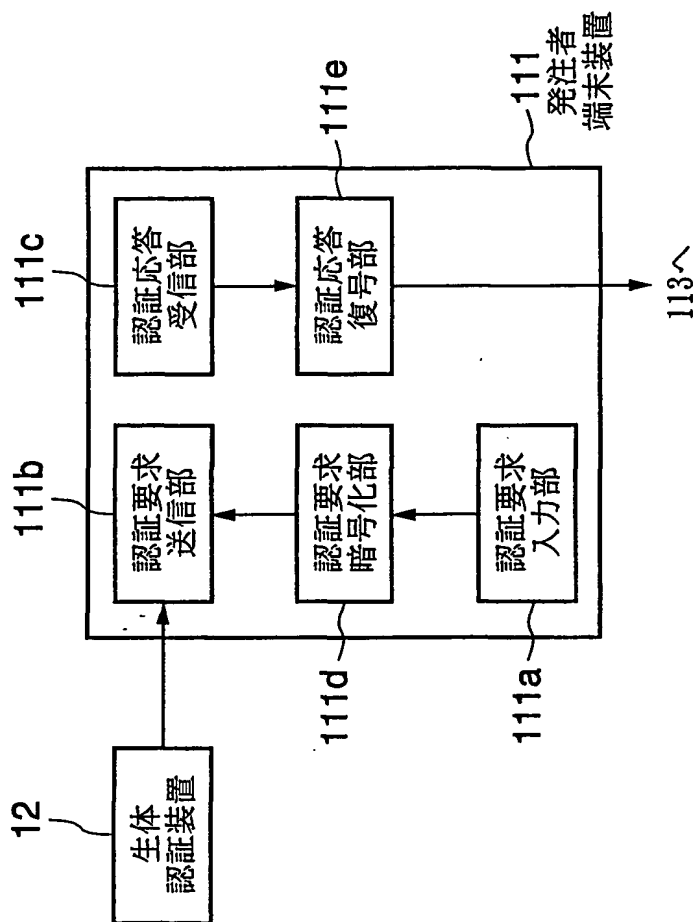
コンピュータで読み取り可能な記録媒体。

FIG.1



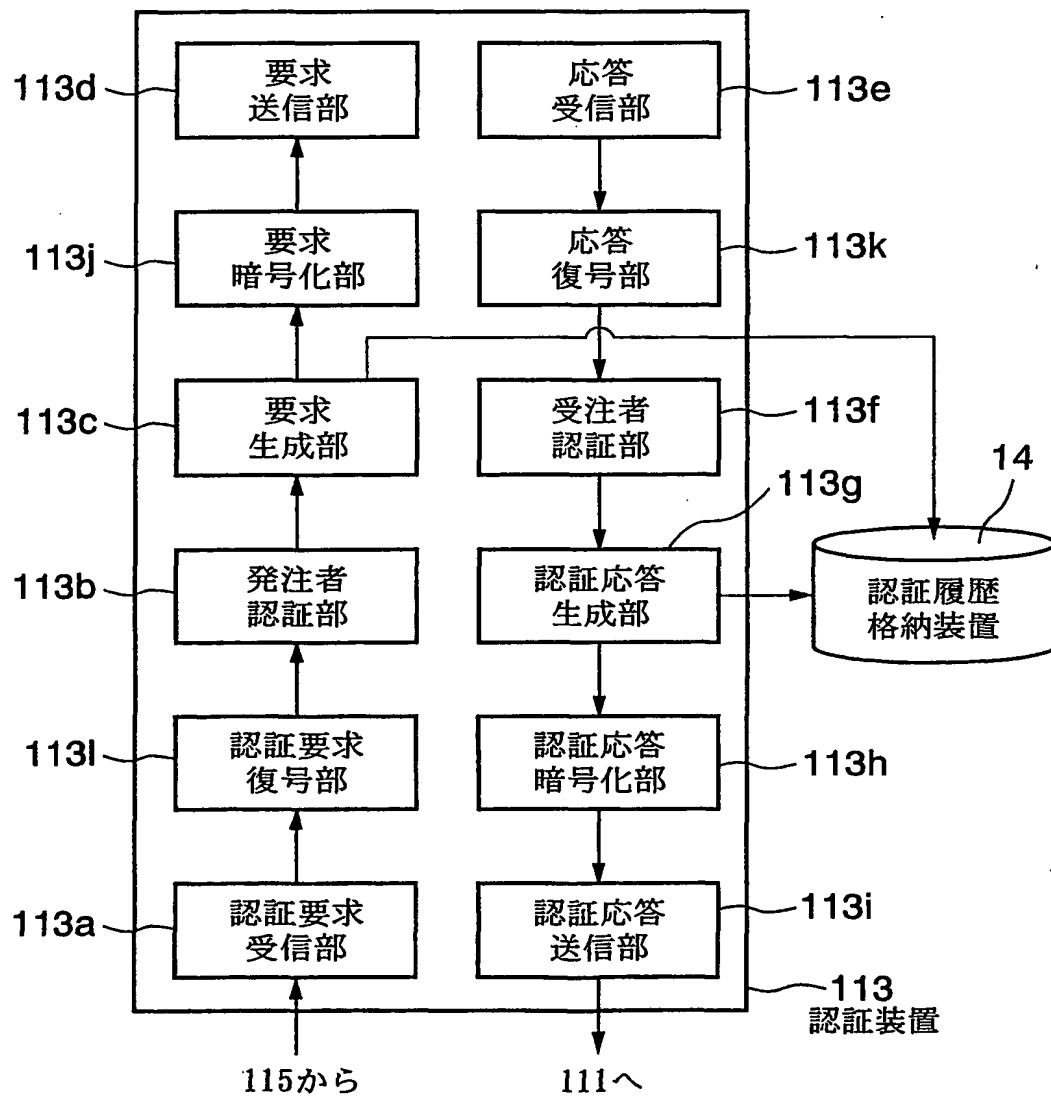
This page Blank (used)

FIG.2



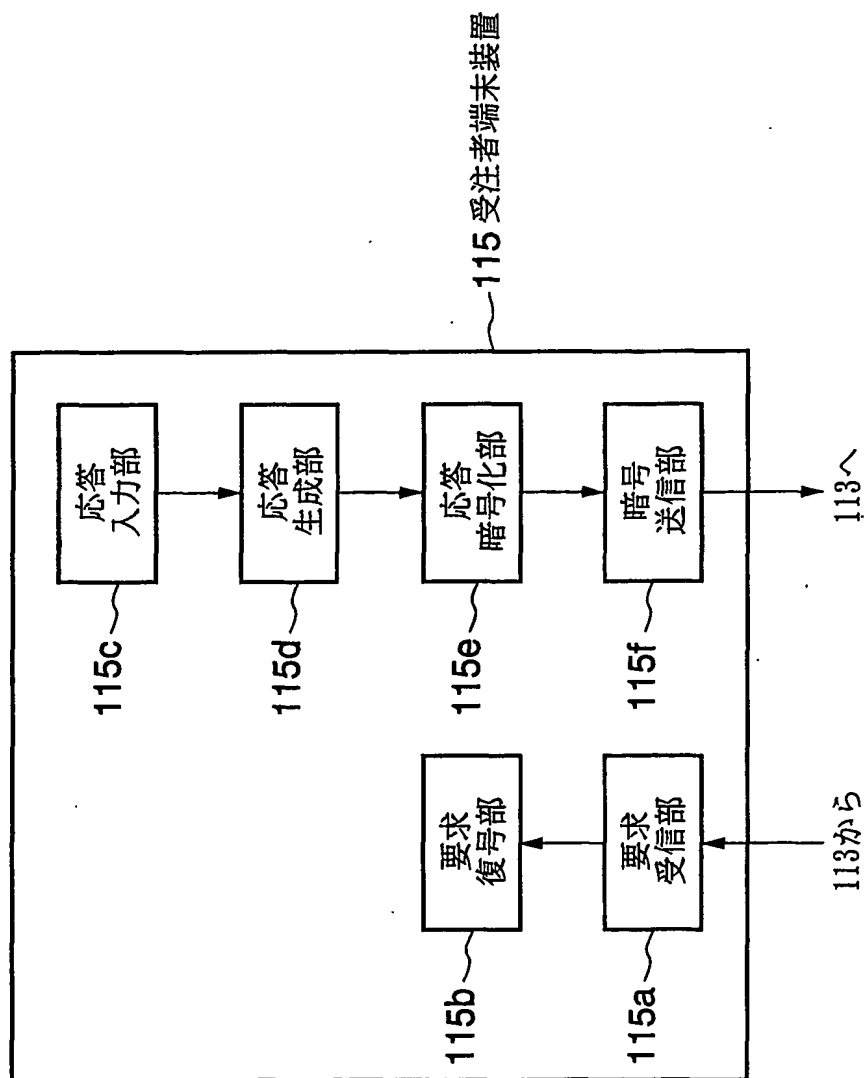
This page Blank (u.s.)

FIG.3



This Page Blank (1/1)

FIG. 4



This Page Blank (1/1)

発注者 受注者
端末装置 111 端末装置 115
認証装置 113

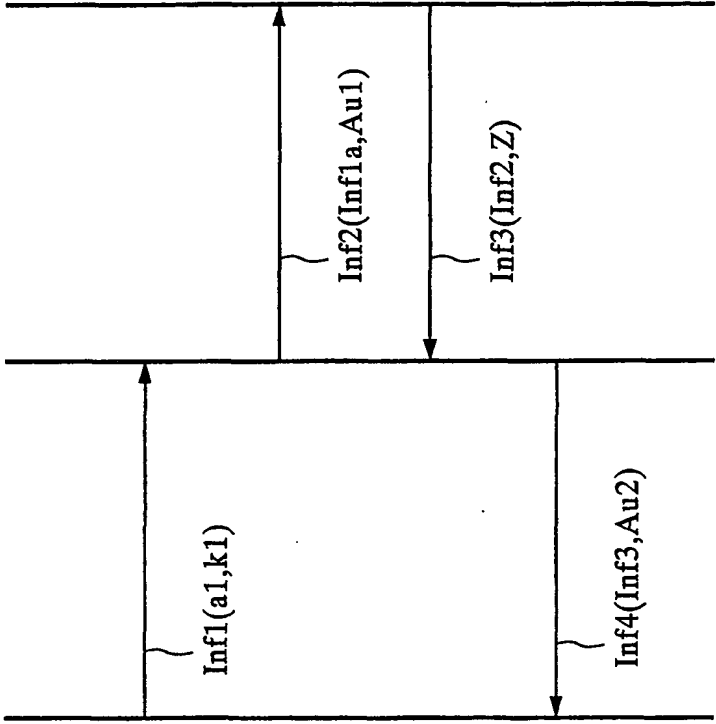


FIG.5A ST11

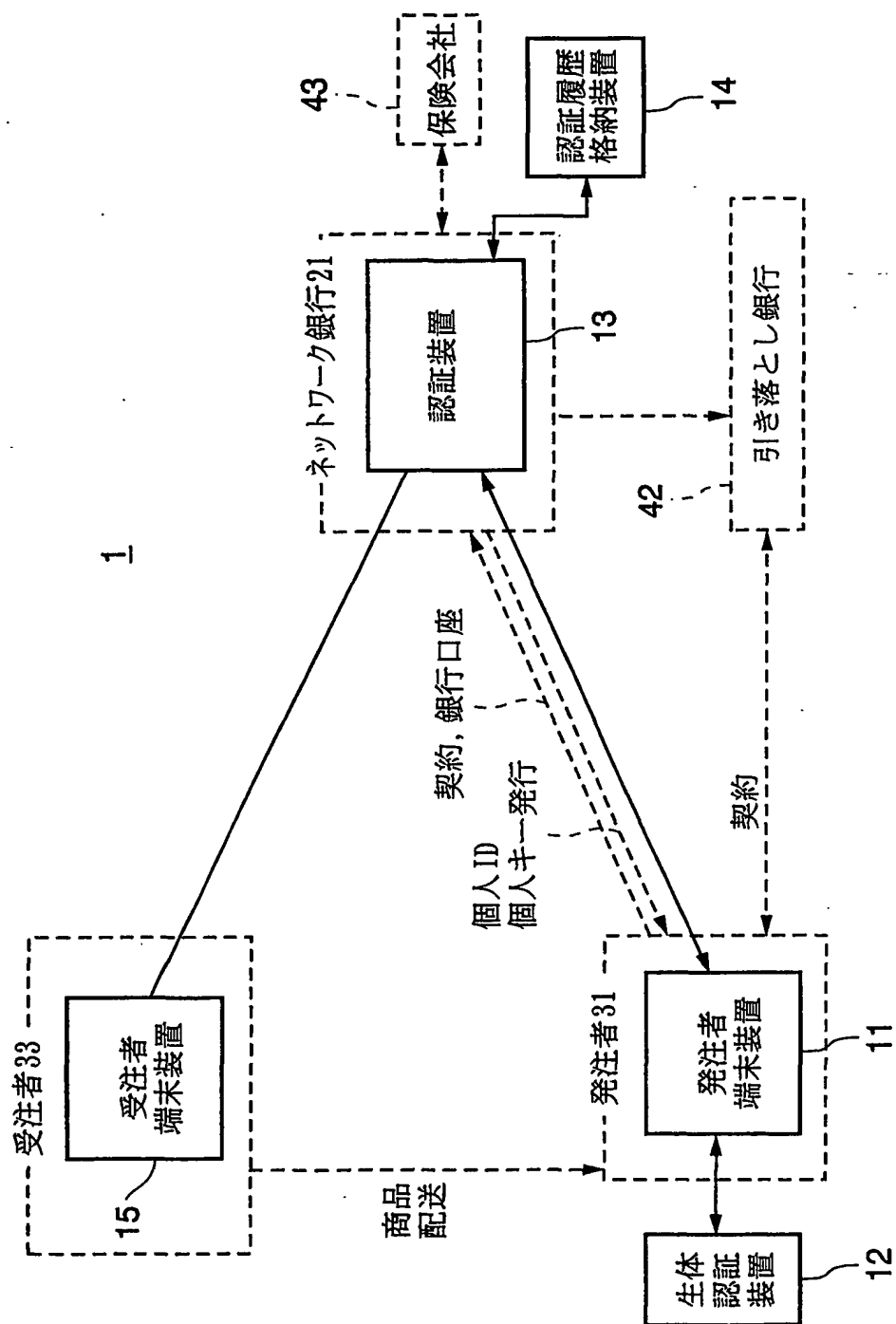
FIG.5B ST12

FIG.5C ST13

FIG.5D ST14

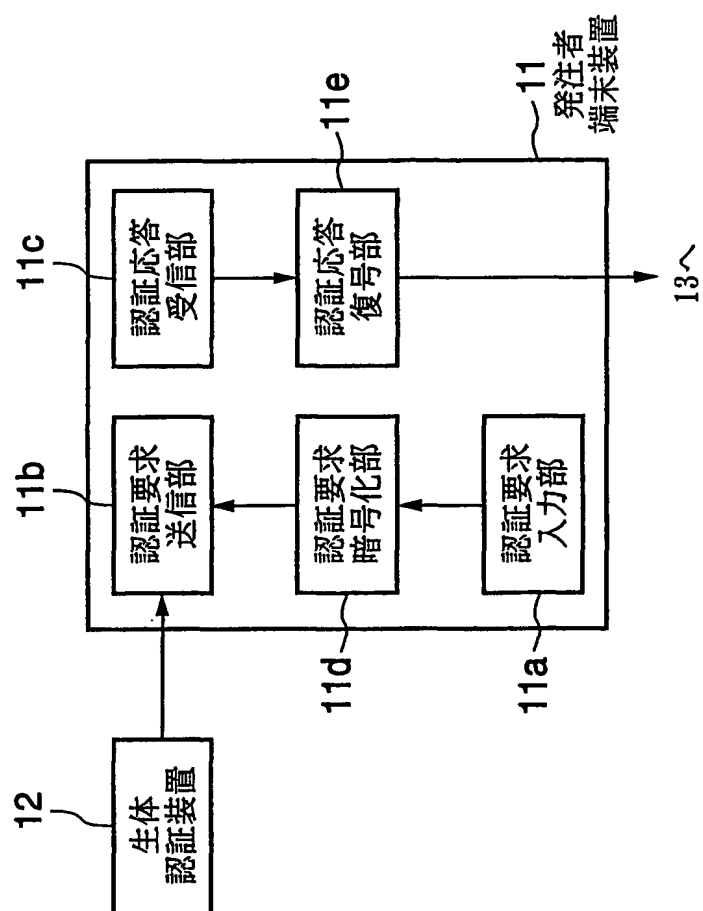
This Page Blank (1/1)

FIG. 6



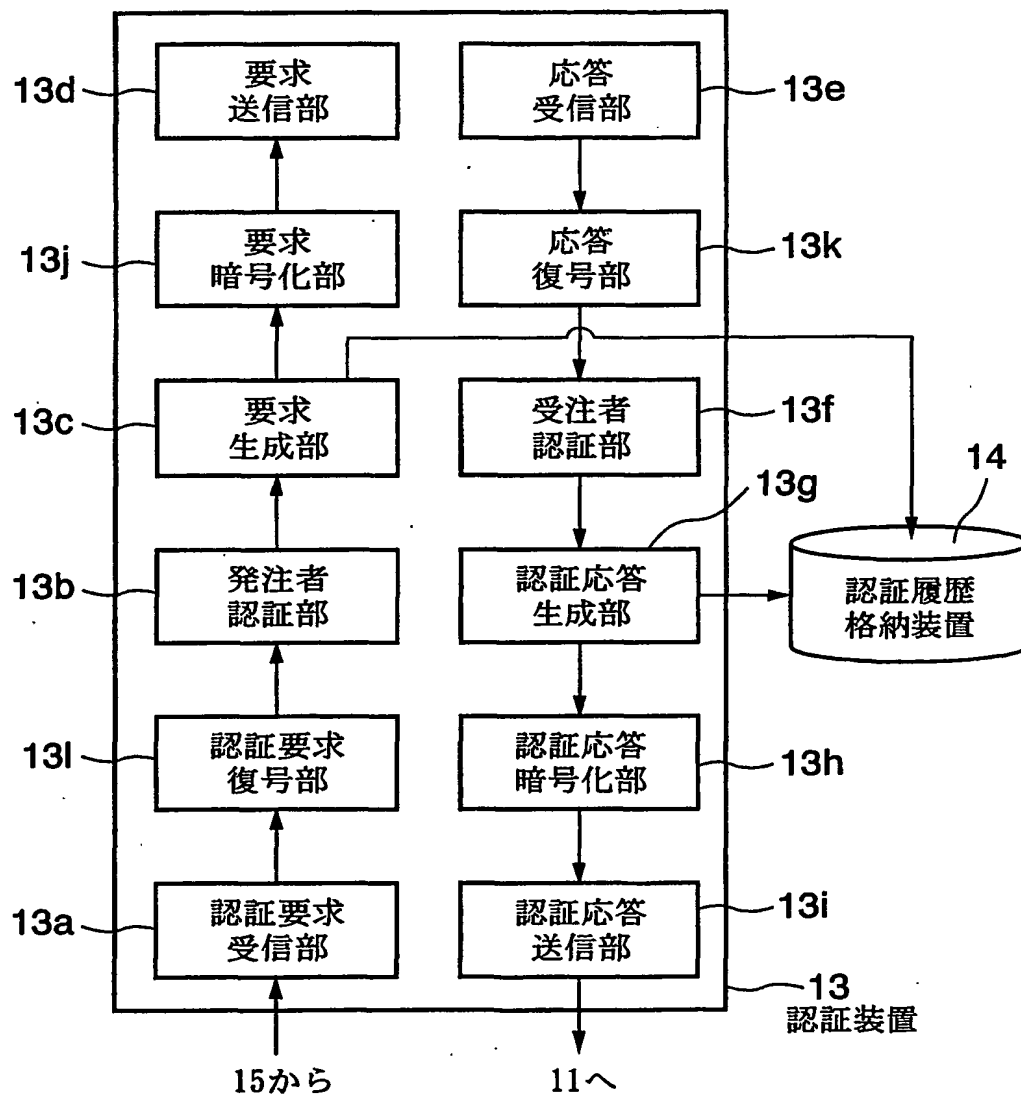
This Page Blank (Page 2)

FIG. 7



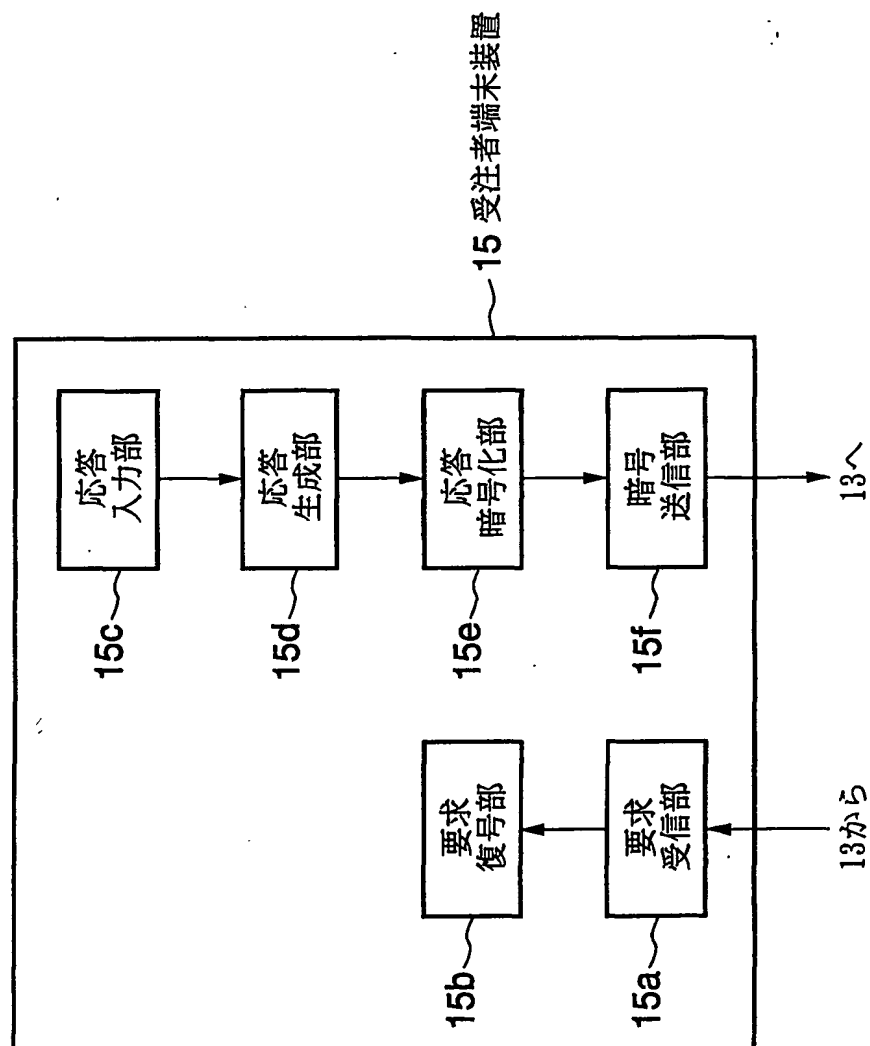
This Page Blank (US Only)

FIG.8



This Page Blank (uspio)

FIG.9



This Page Blank (uspio)

発注者
端末装置11

認証装置
13

受注者
端末装置15

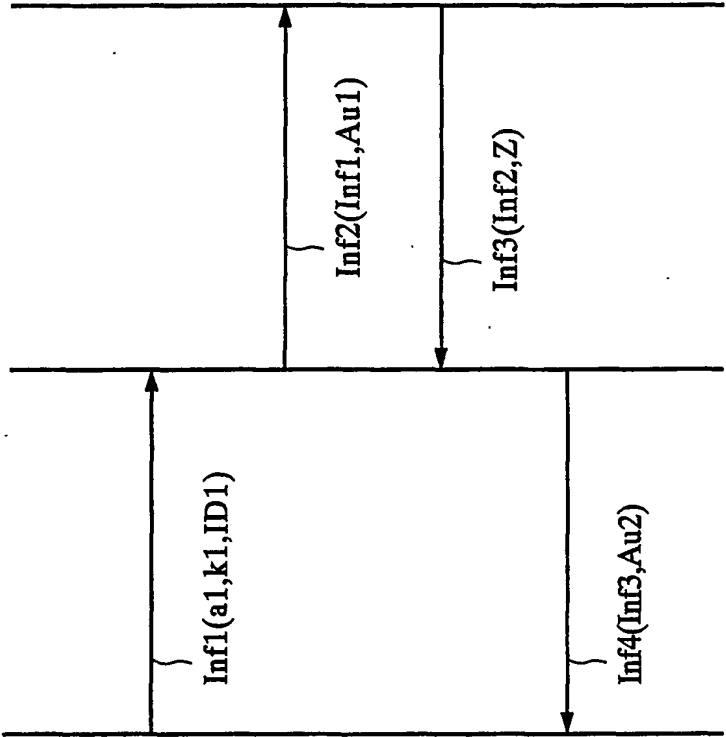


FIG.10A ST1

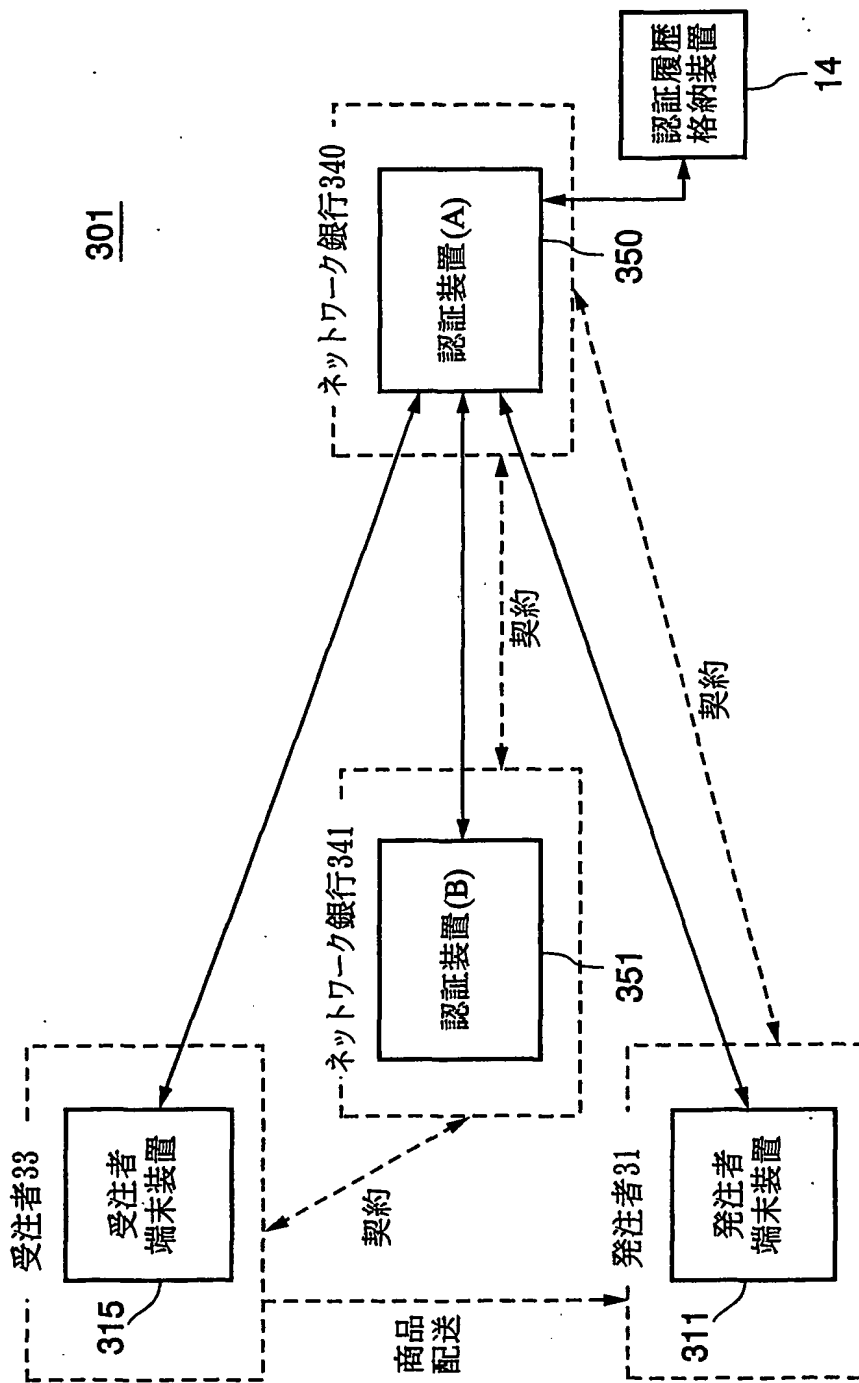
FIG.10B ST2

FIG.10C ST3

FIG.10D ST4

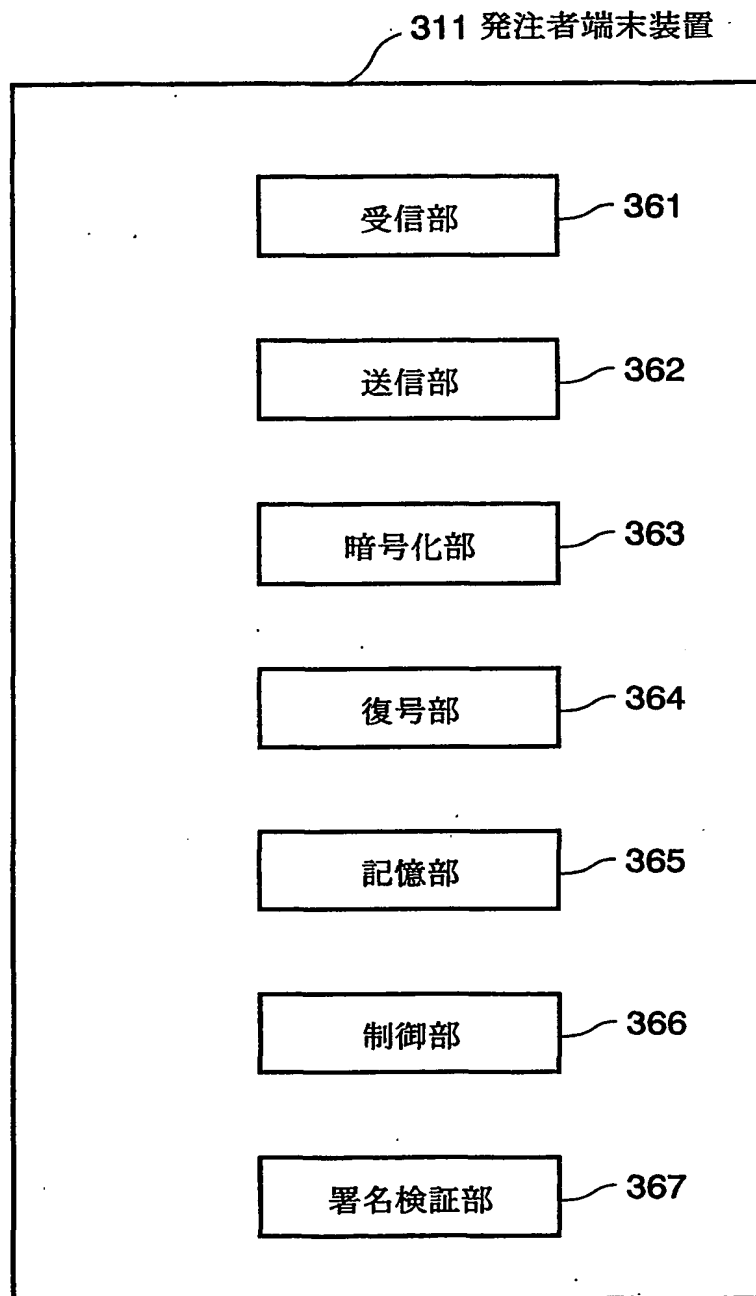
This Page Blank (uspio)

FIG.11



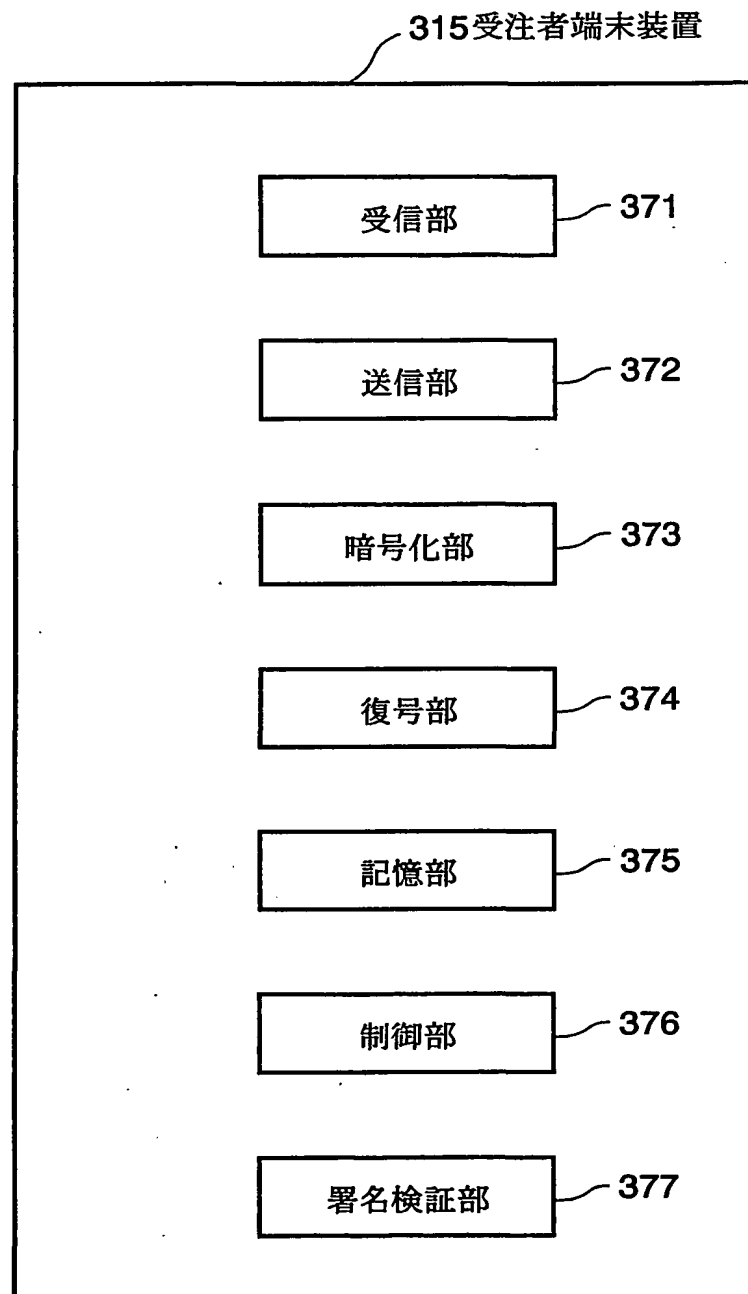
This Page Blank (uspto)

FIG.12



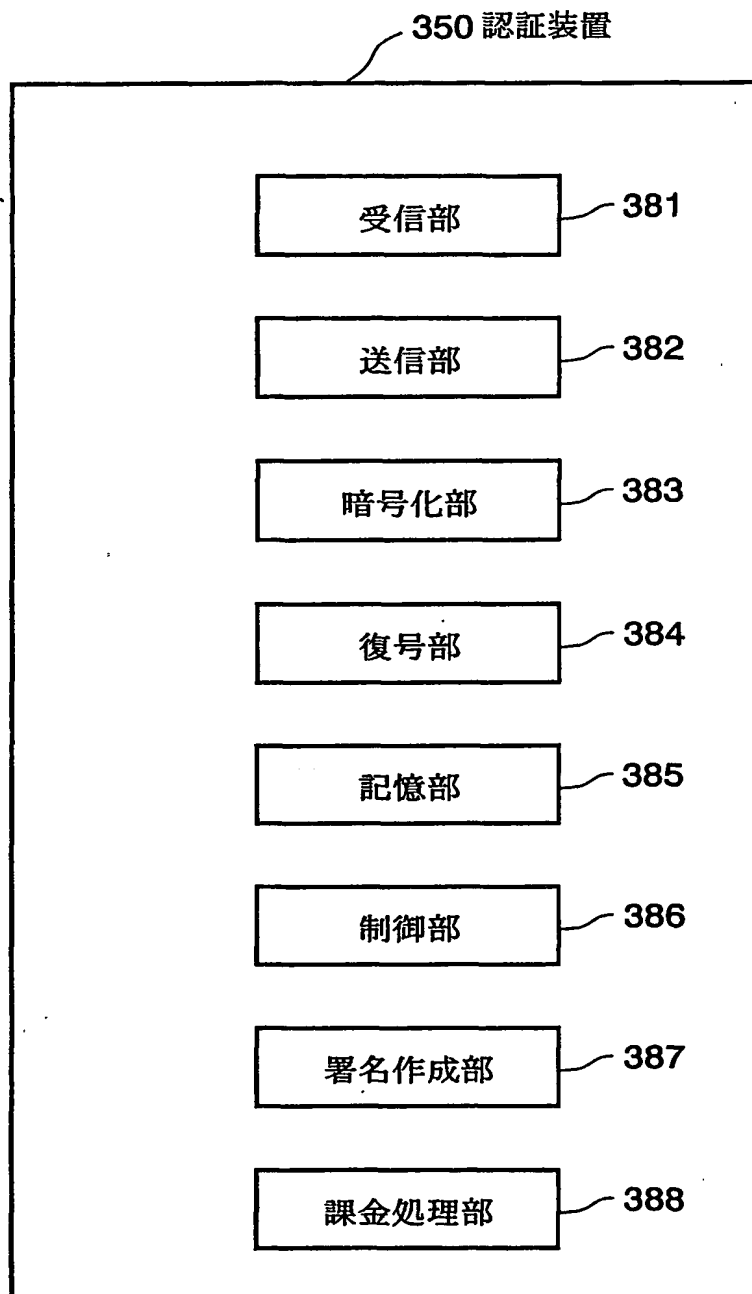
This page Blank (Page 1)

FIG.13



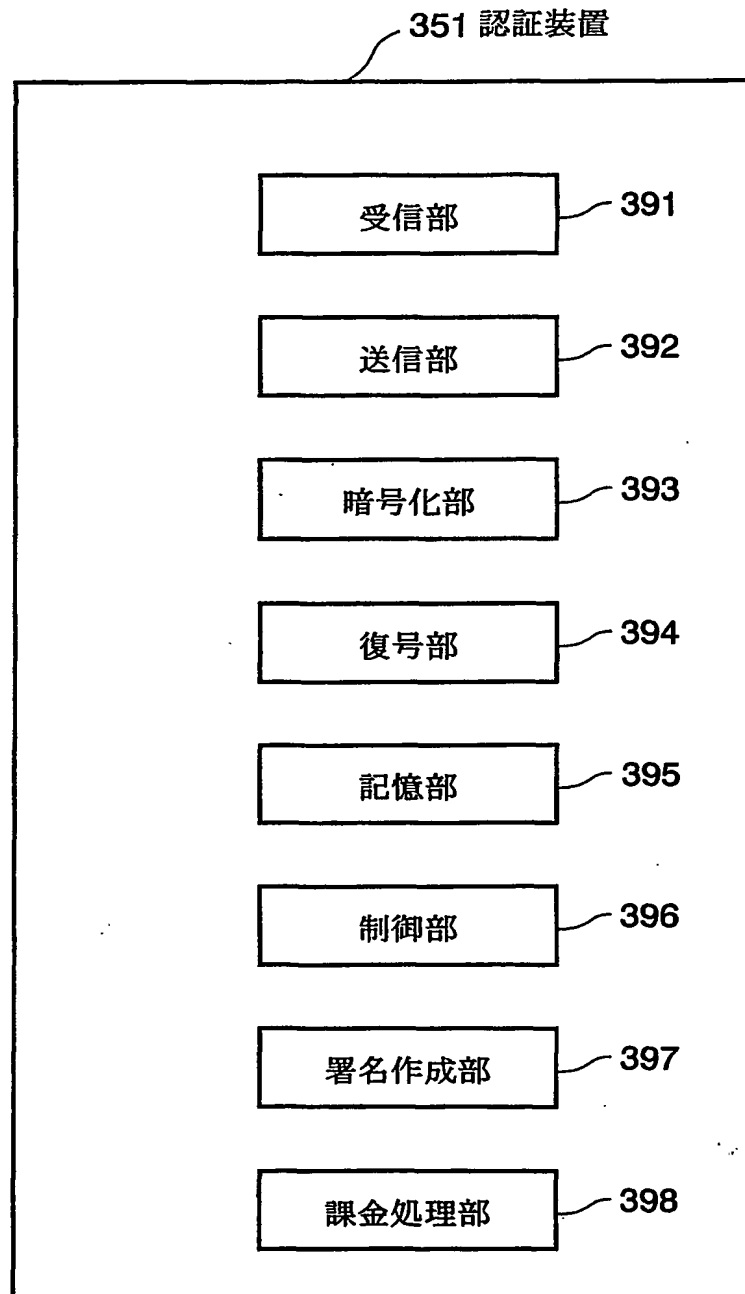
This page Blank (1)

FIG.14



This Page Blank (Page 1)

FIG.15



This Page Blank (Upper)

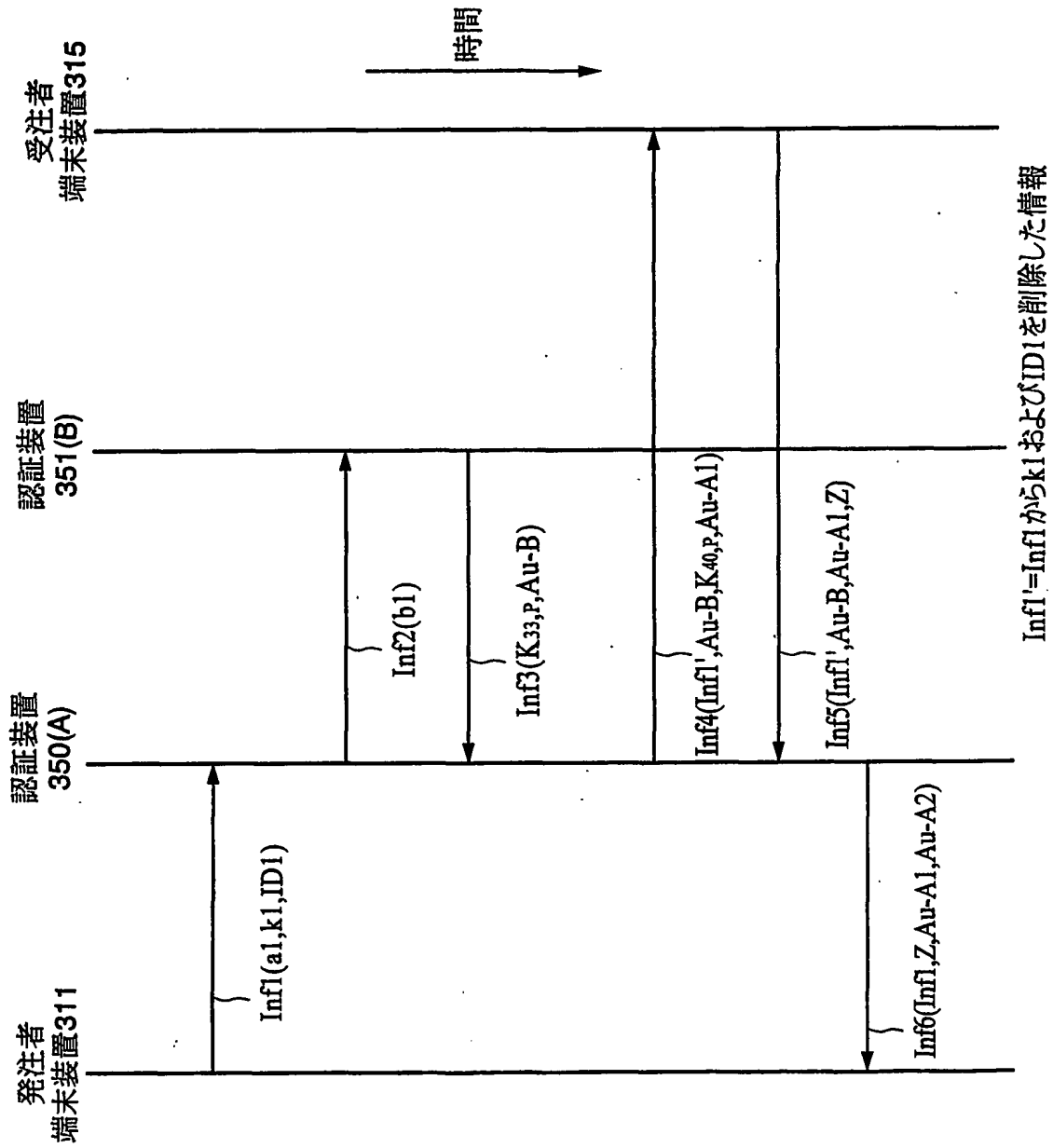


FIG.16A ST31

FIG.16B ST32

FIG.16C ST33

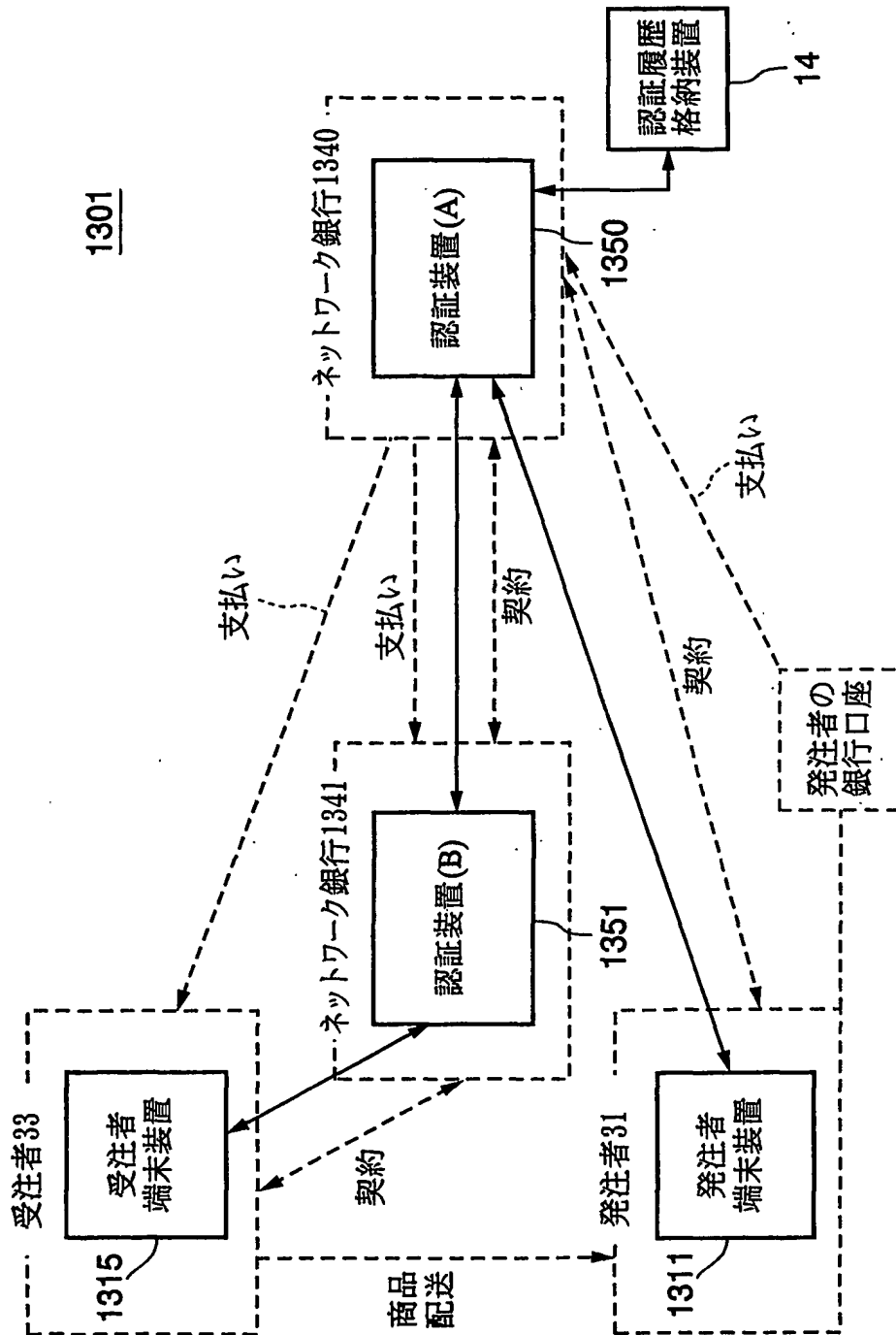
FIG.16D ST34

FIG.16E ST35

FIG.16F ST36

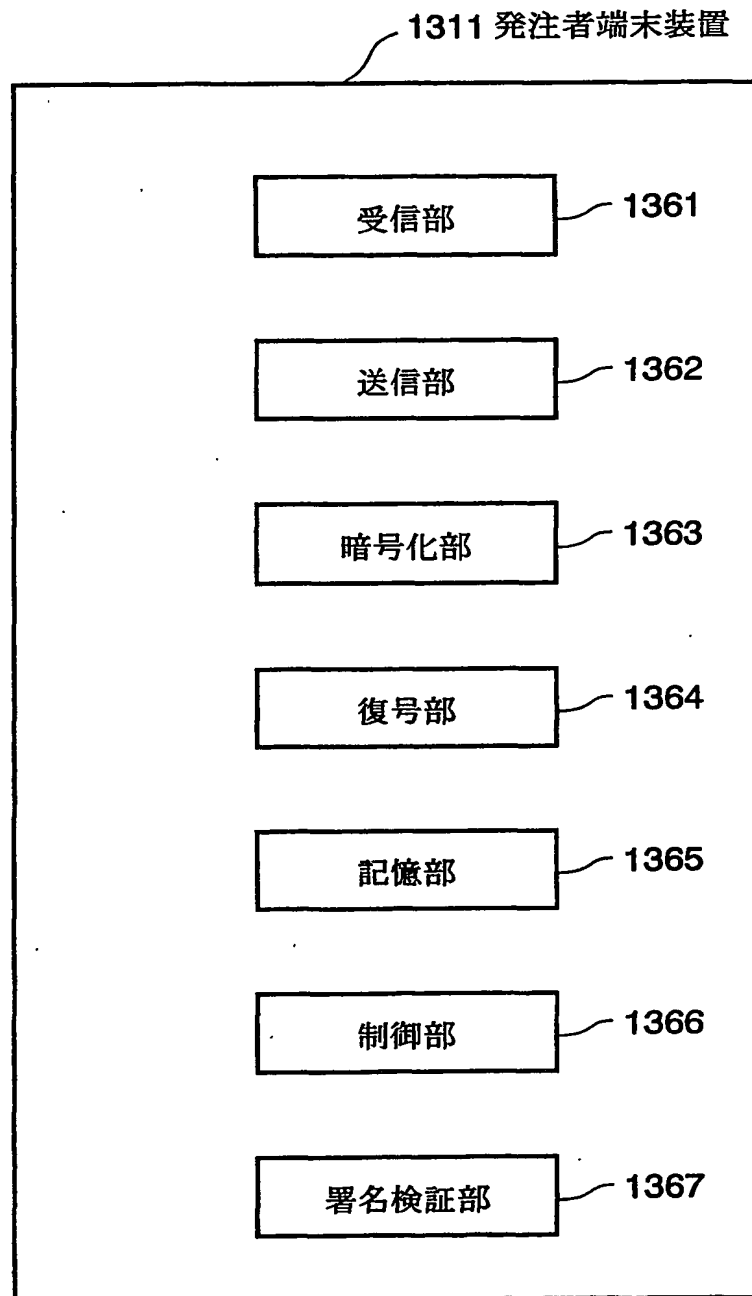
This Page Blank (1/30/97)

FIG.17



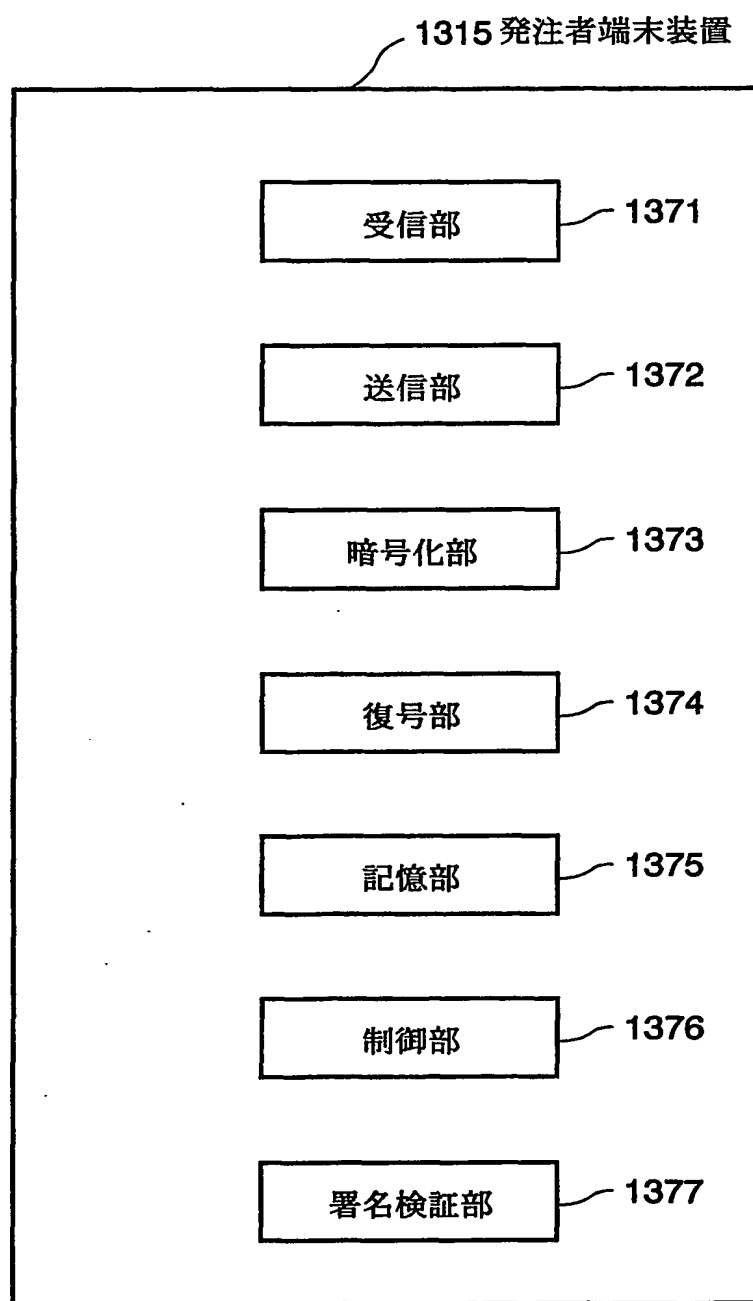
This Page Blank (USP10)

FIG.18



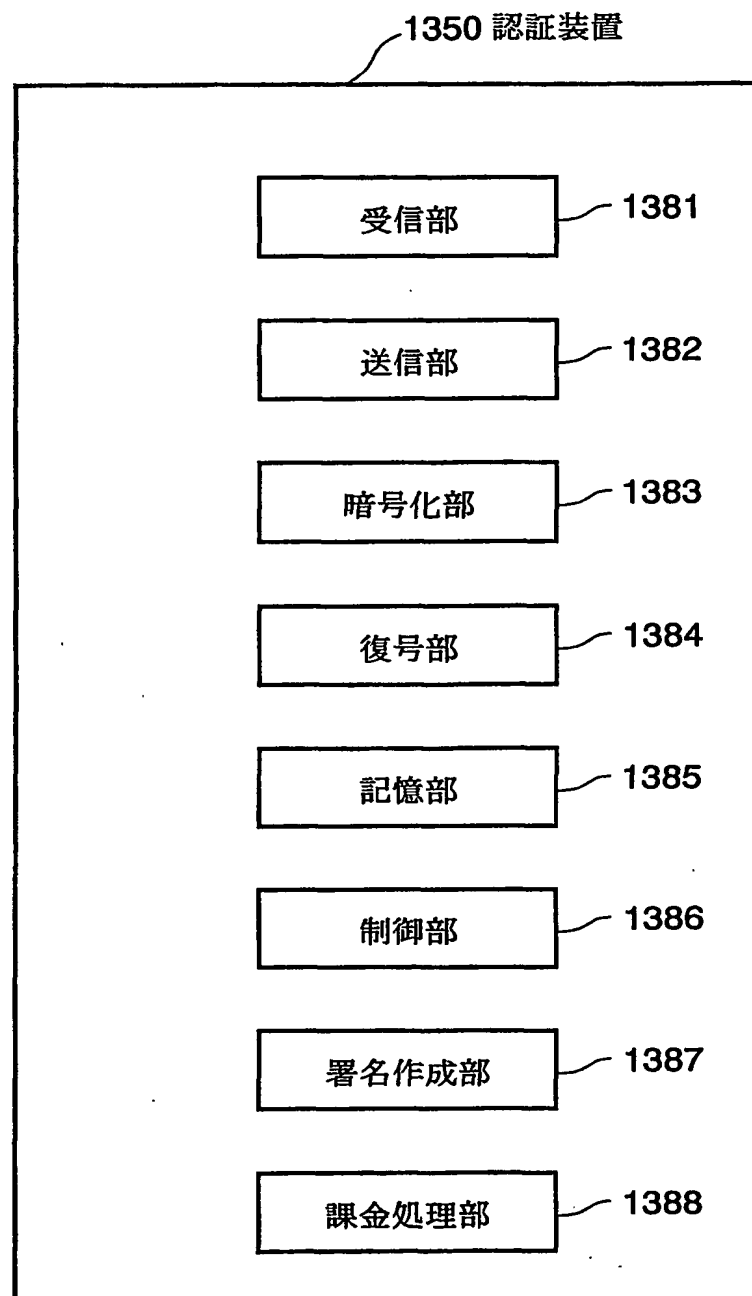
This Page Blank (uspia)

FIG.19



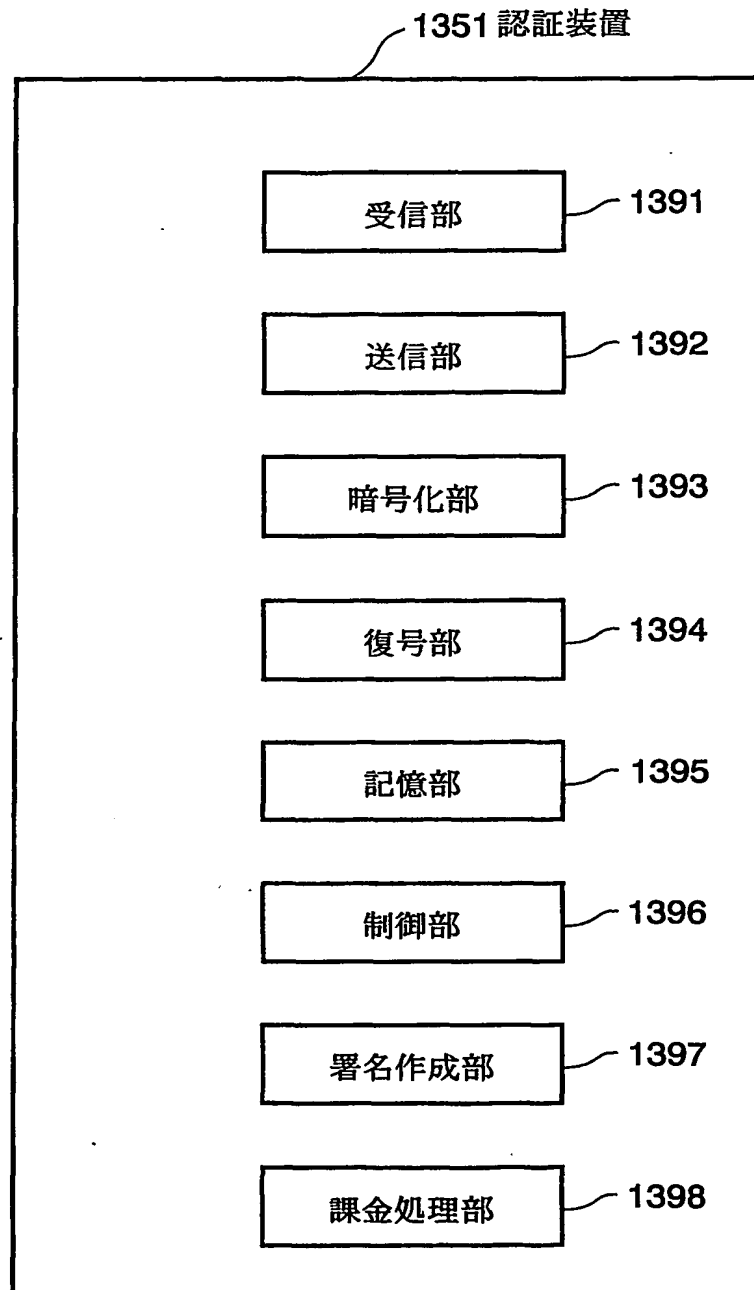
This Page Blank (uspto)

FIG.20

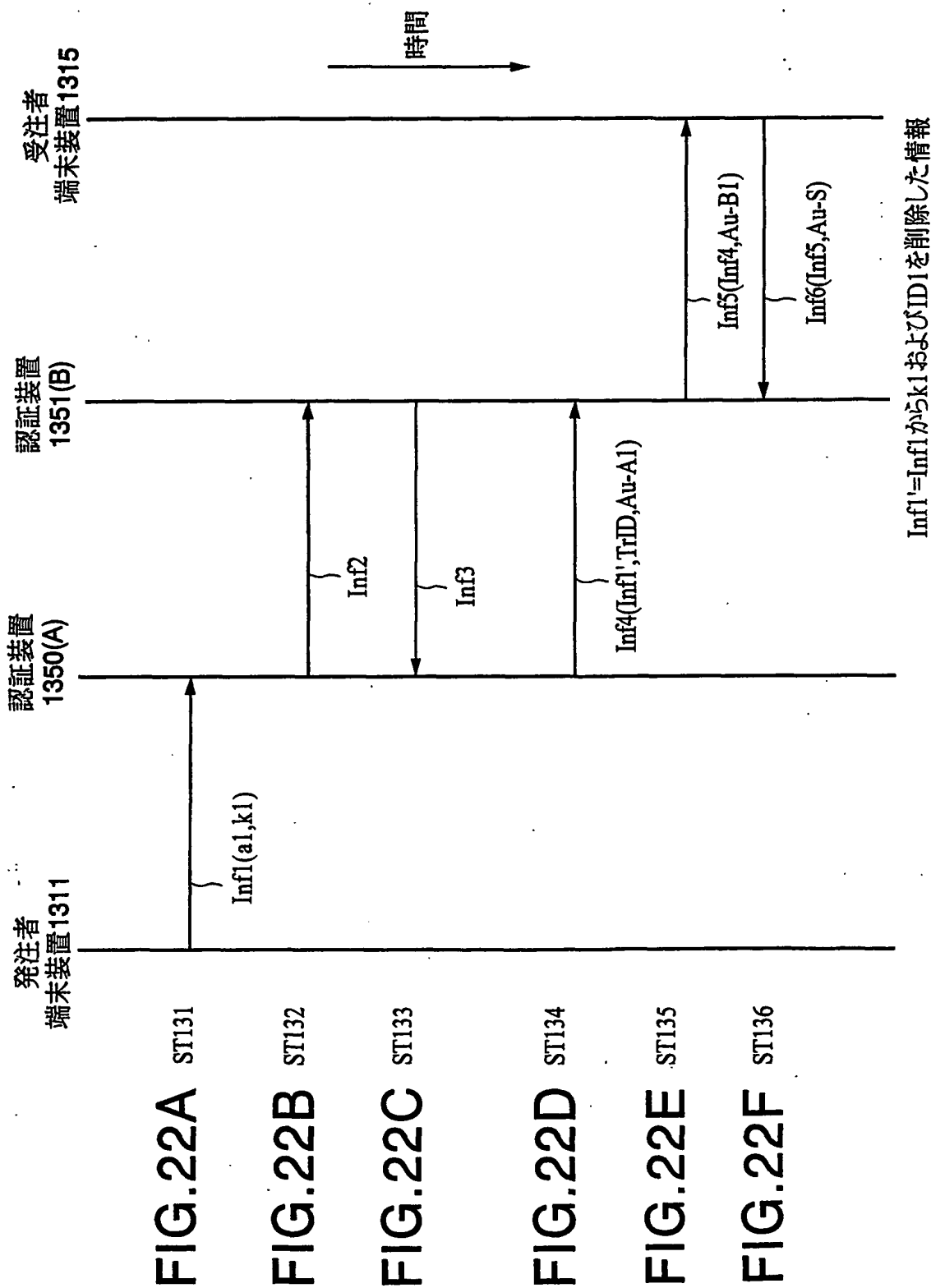


This Page Blank (USP 201)

FIG.21



This page Blank (uspl.)



This Page Blank (USP 271)

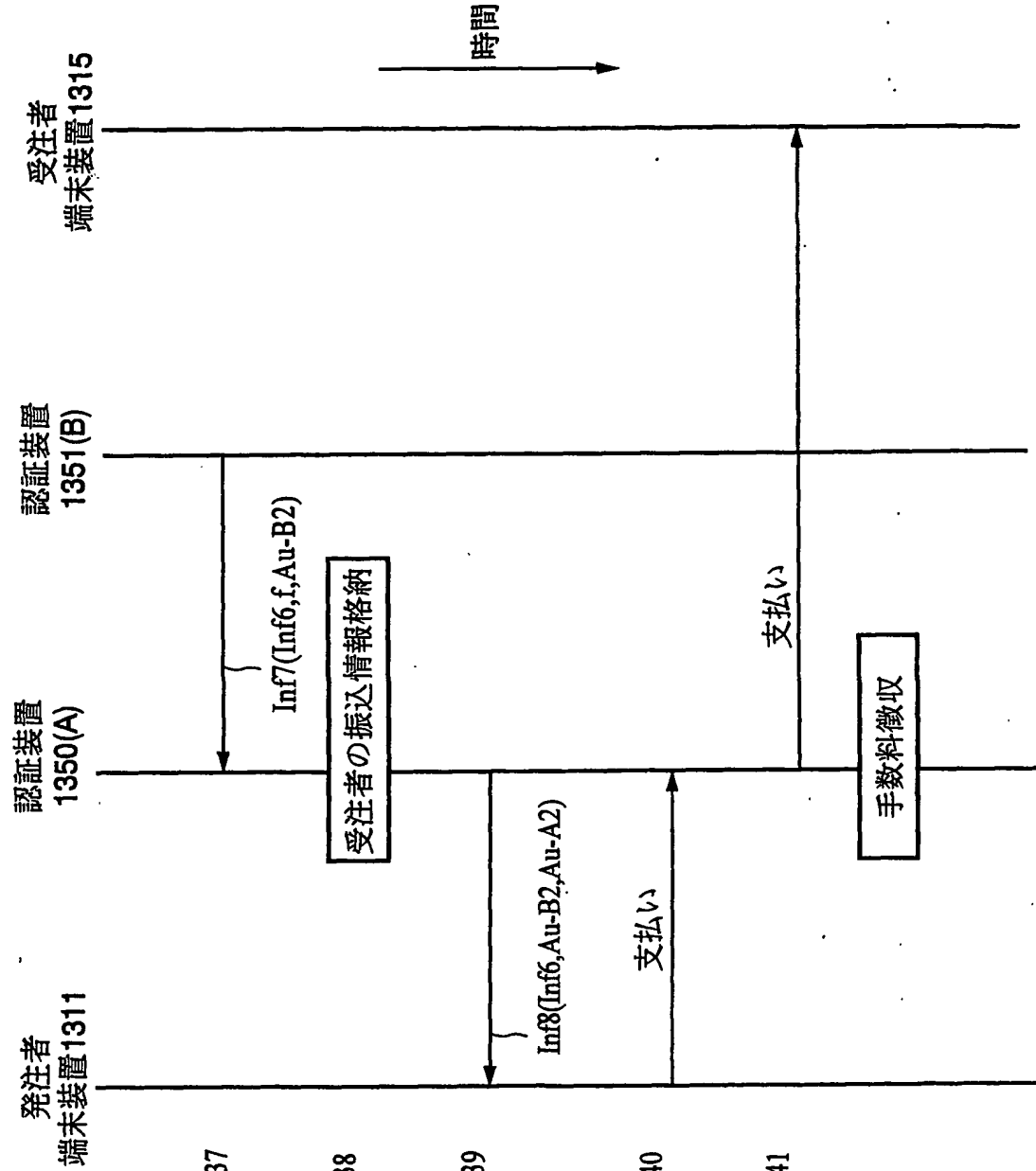


FIG.23A

FIG.23B

FIG.23C

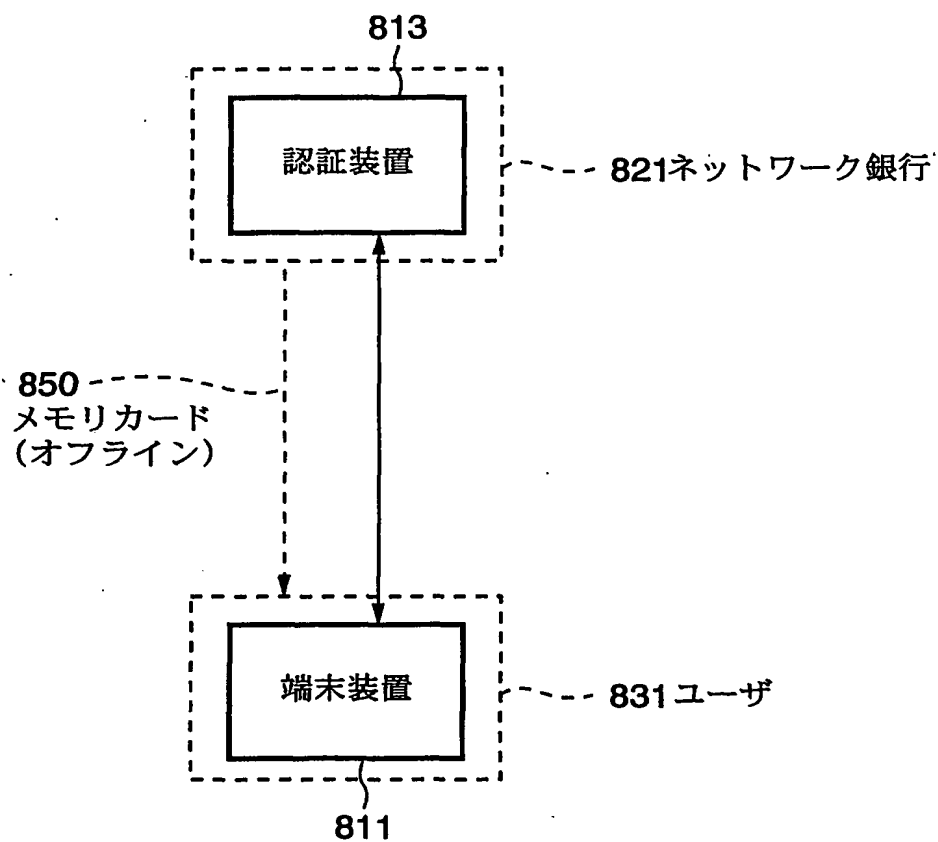
FIG.23D

FIG.23E

FIG.23F

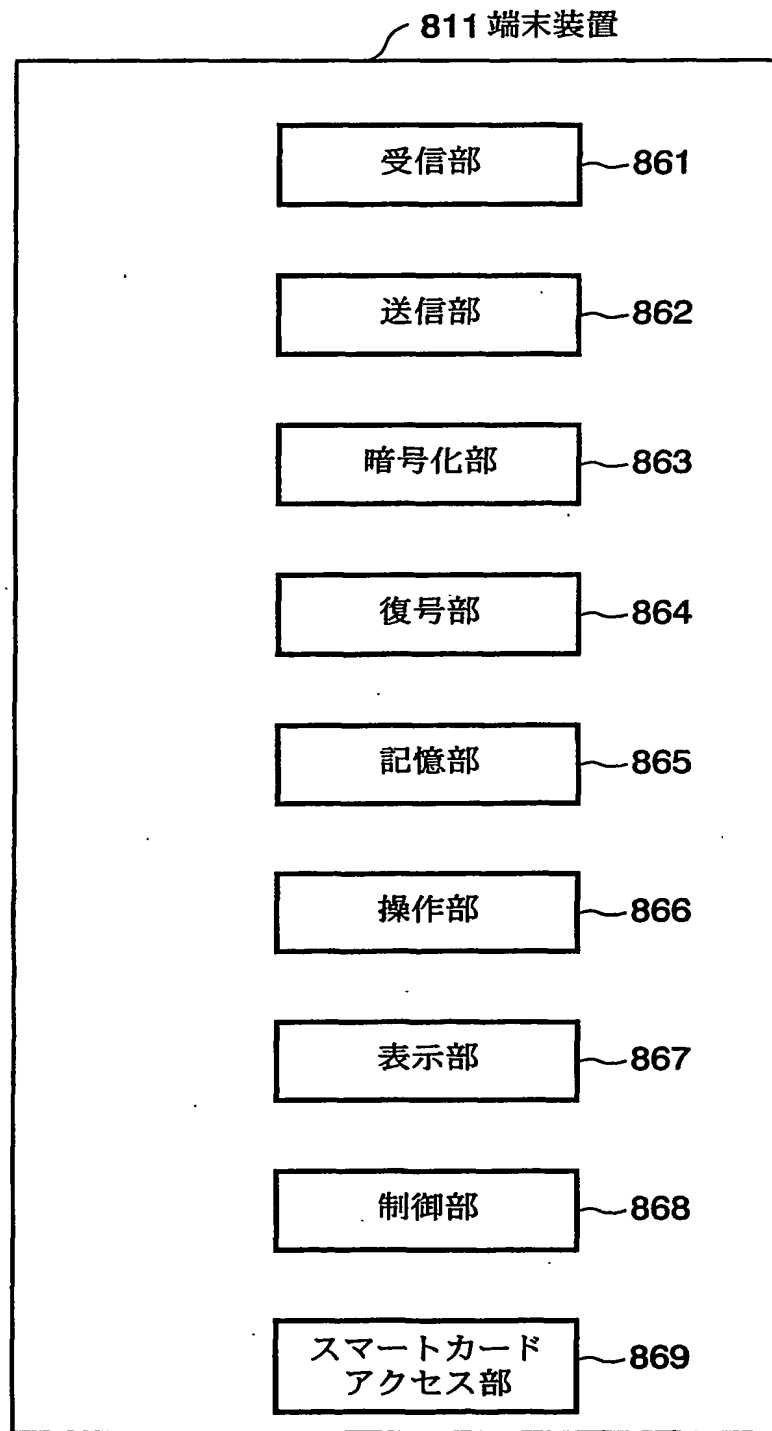
This page Blank (4/25/2022)

FIG.24

801

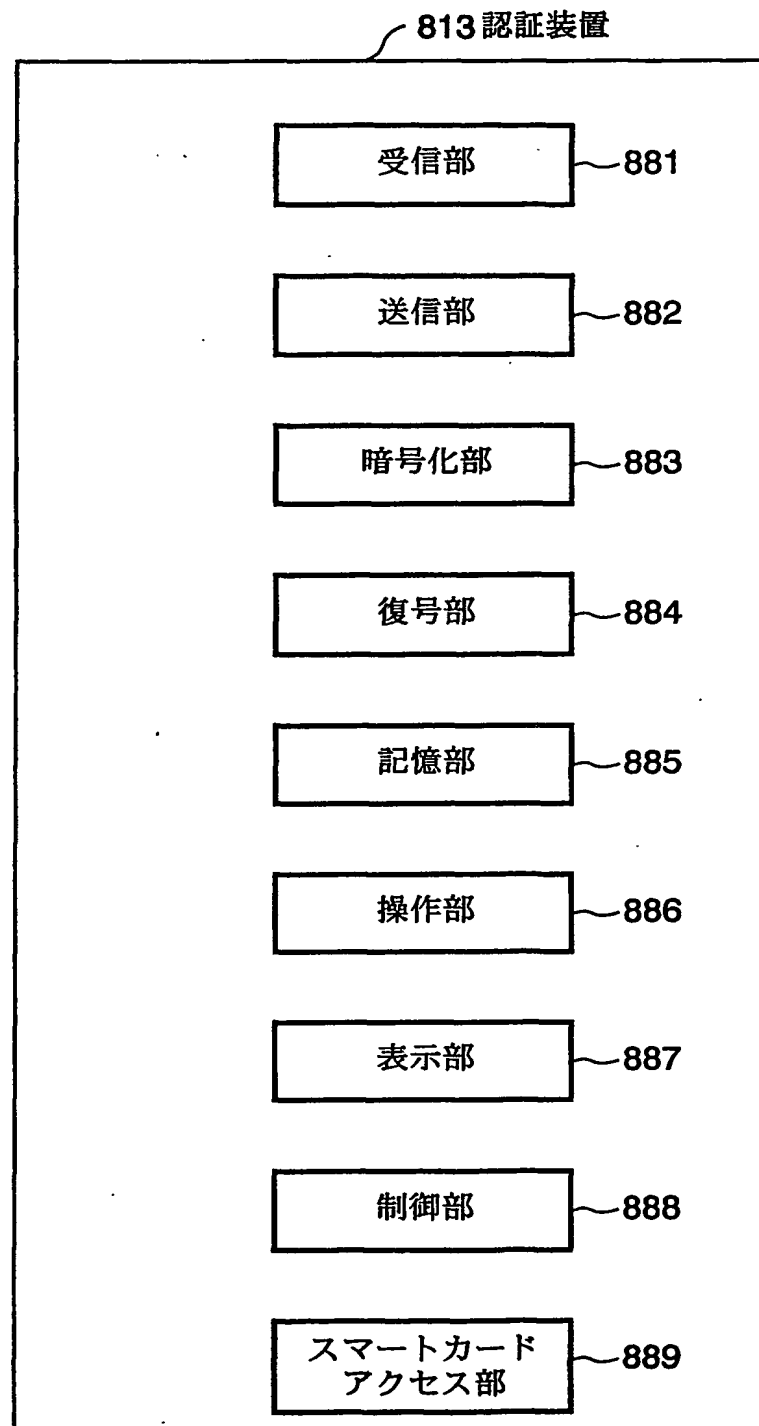
This page Blank (1/20/2024)

FIG.25



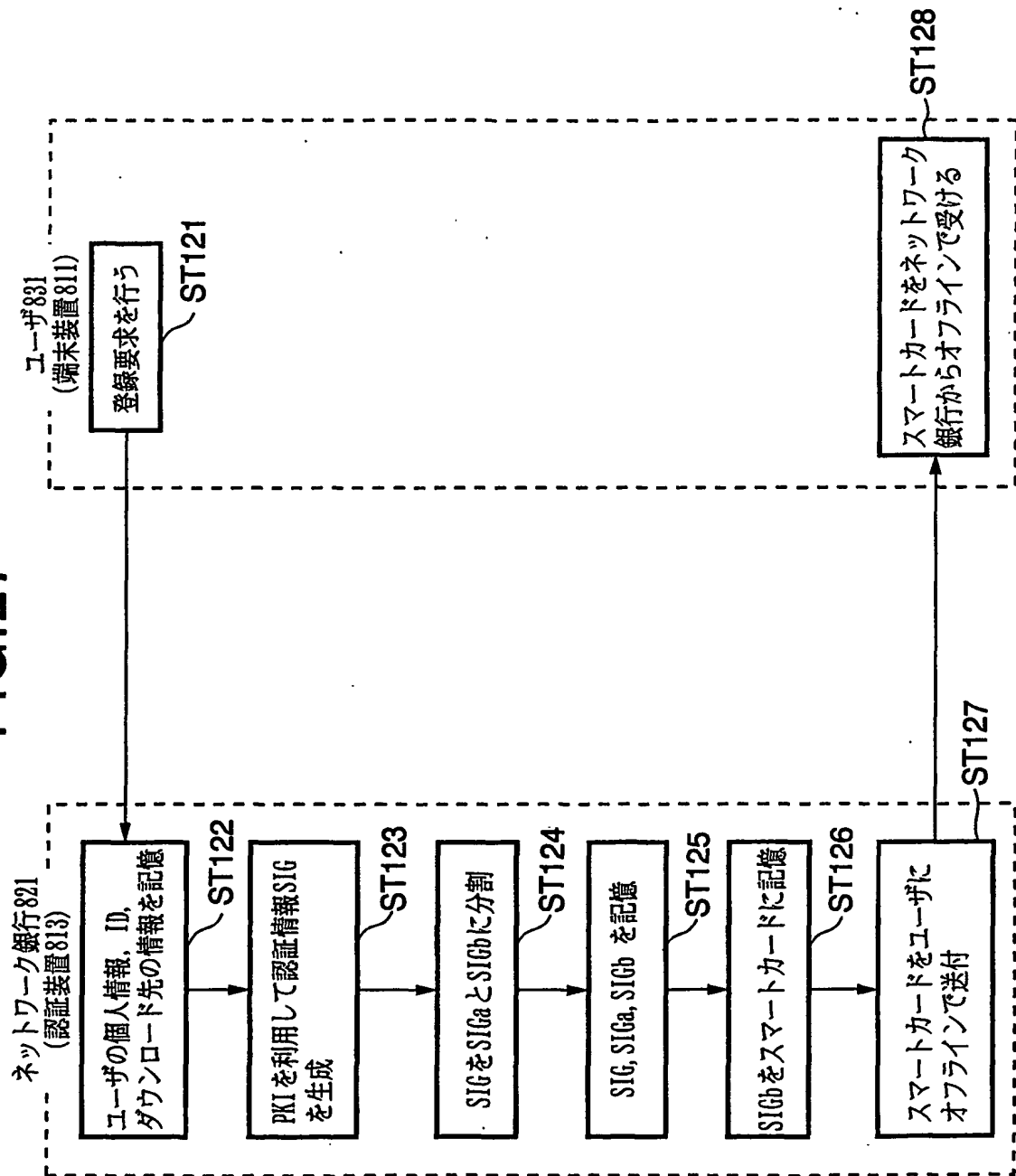
This page Blank (Page 2)

FIG.26



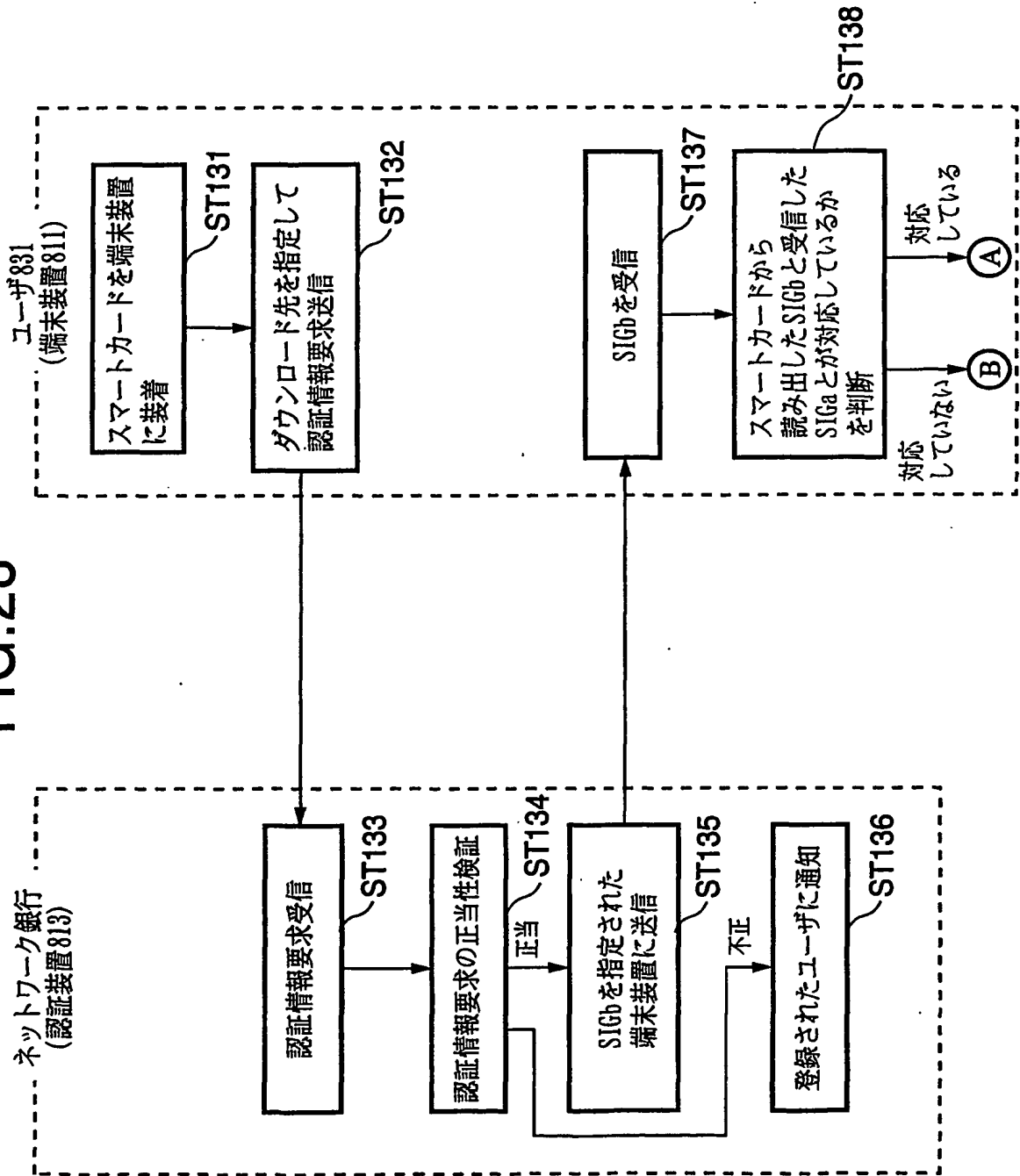
This Page Blank (uspi07)

FIG. 27



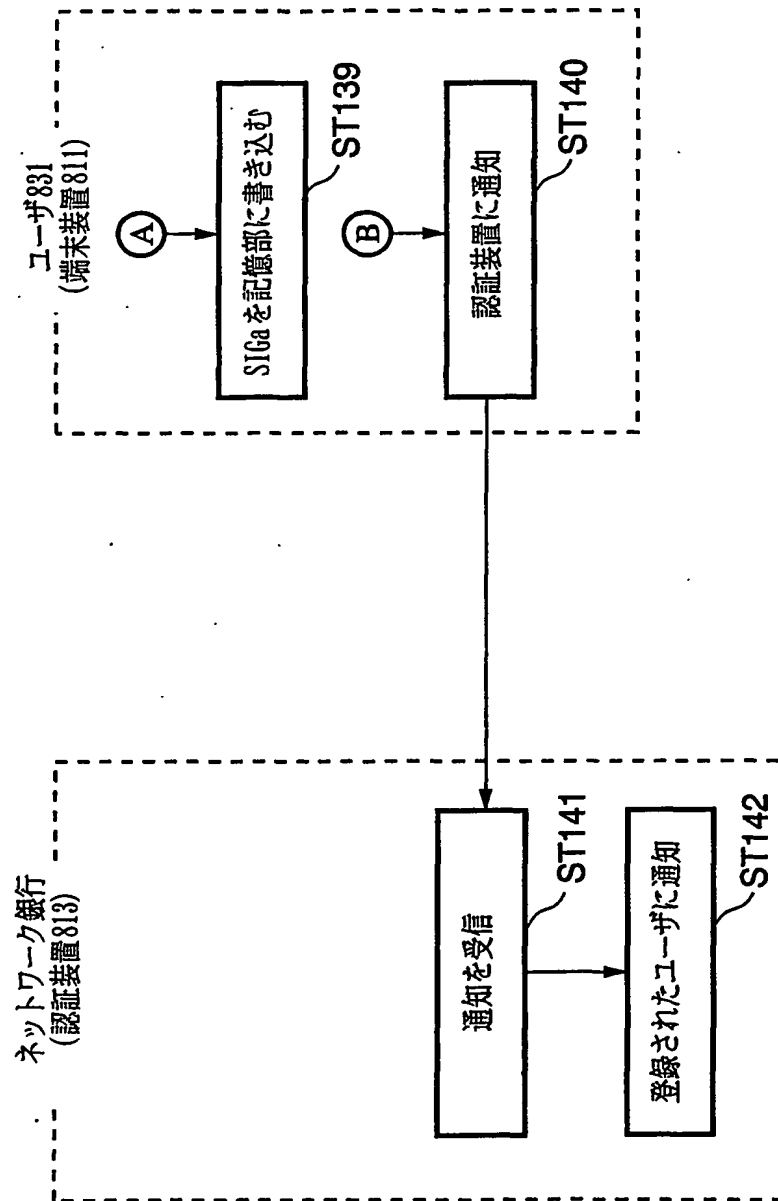
This Page Blank (uspio)

FIG. 28



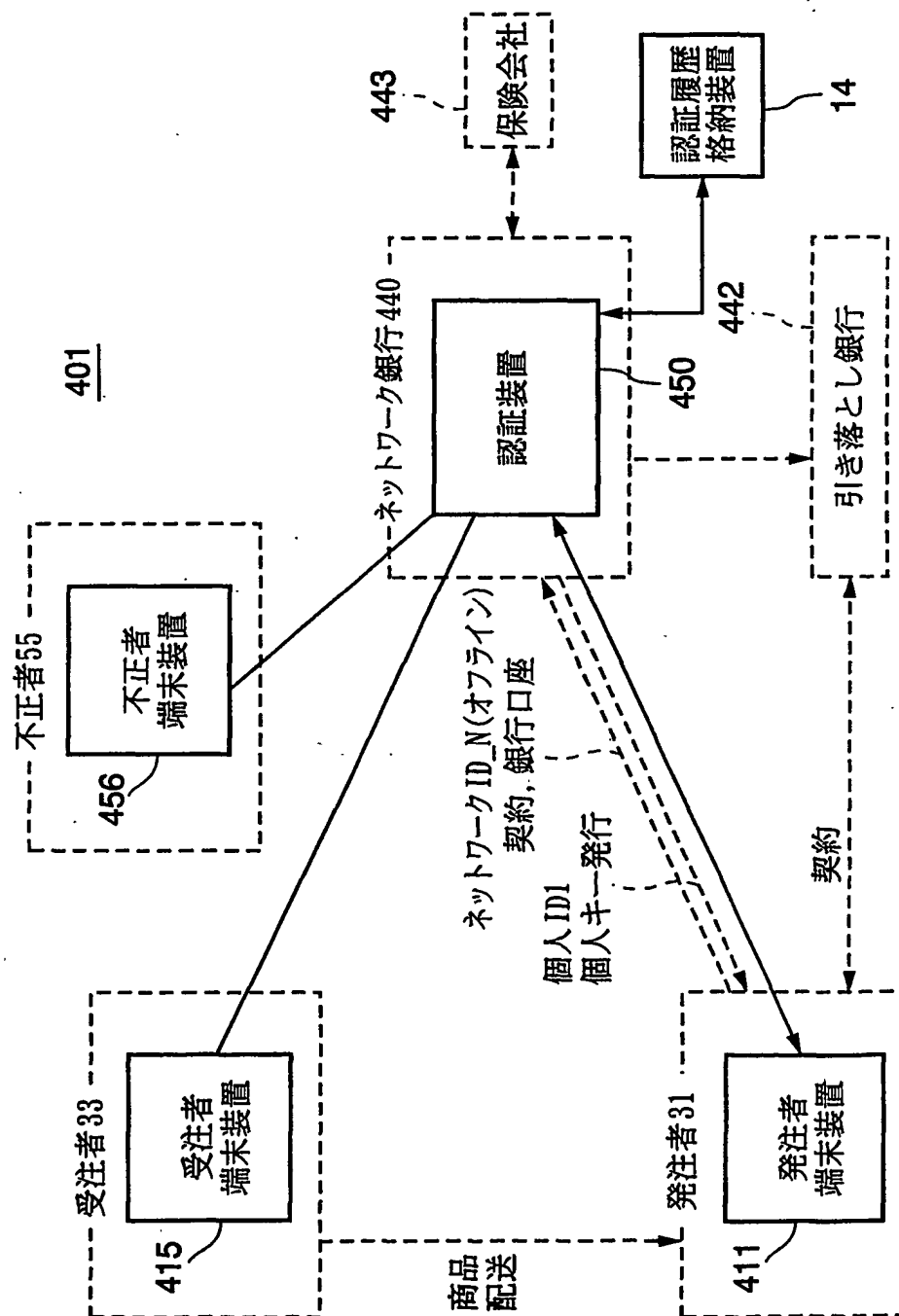
This Page Blank (uspto)

FIG.29



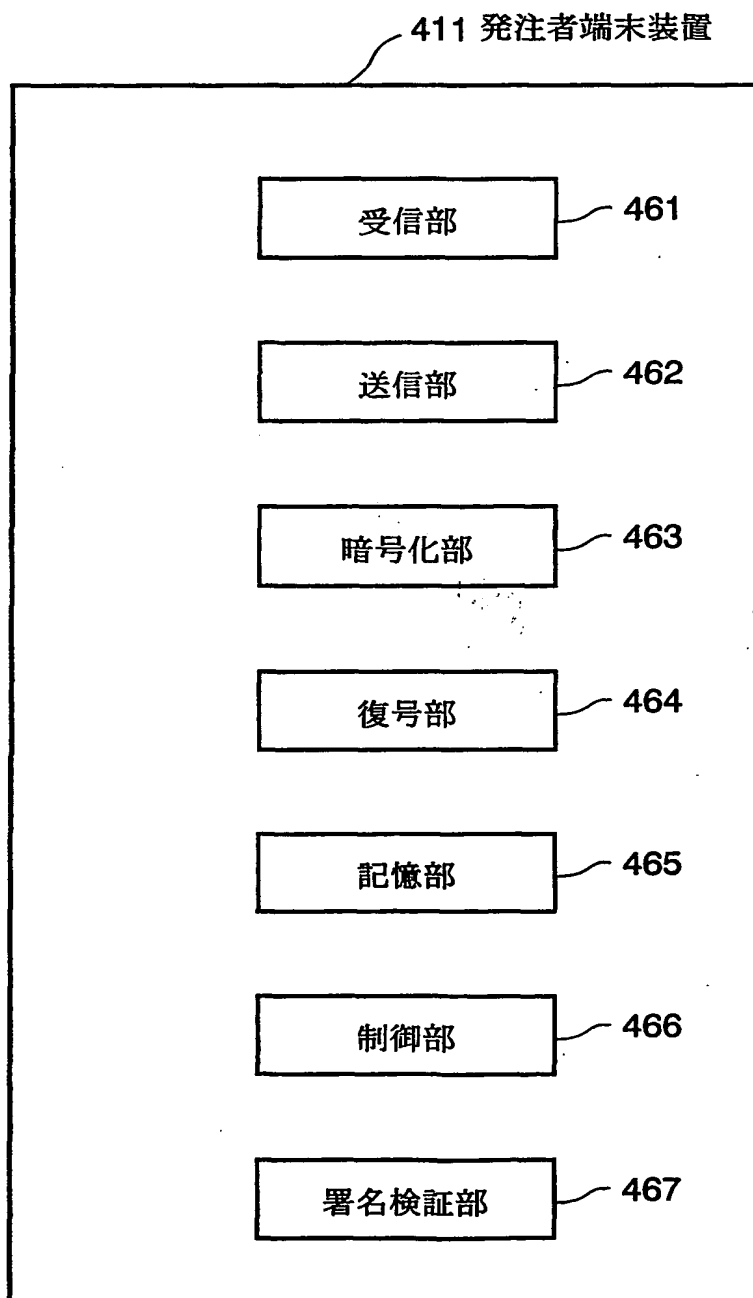
This Page Blank (USP10)

FIG. 30



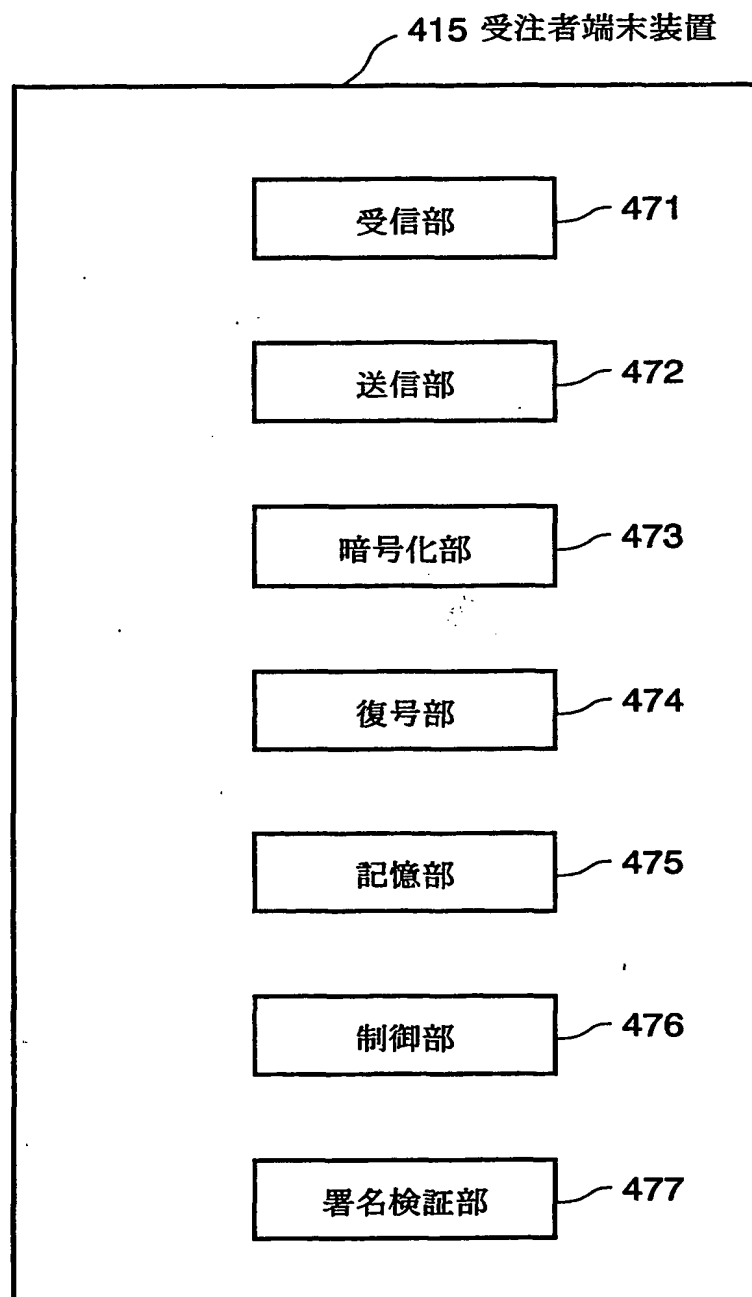
This Page Blank (USP 112)

FIG.31



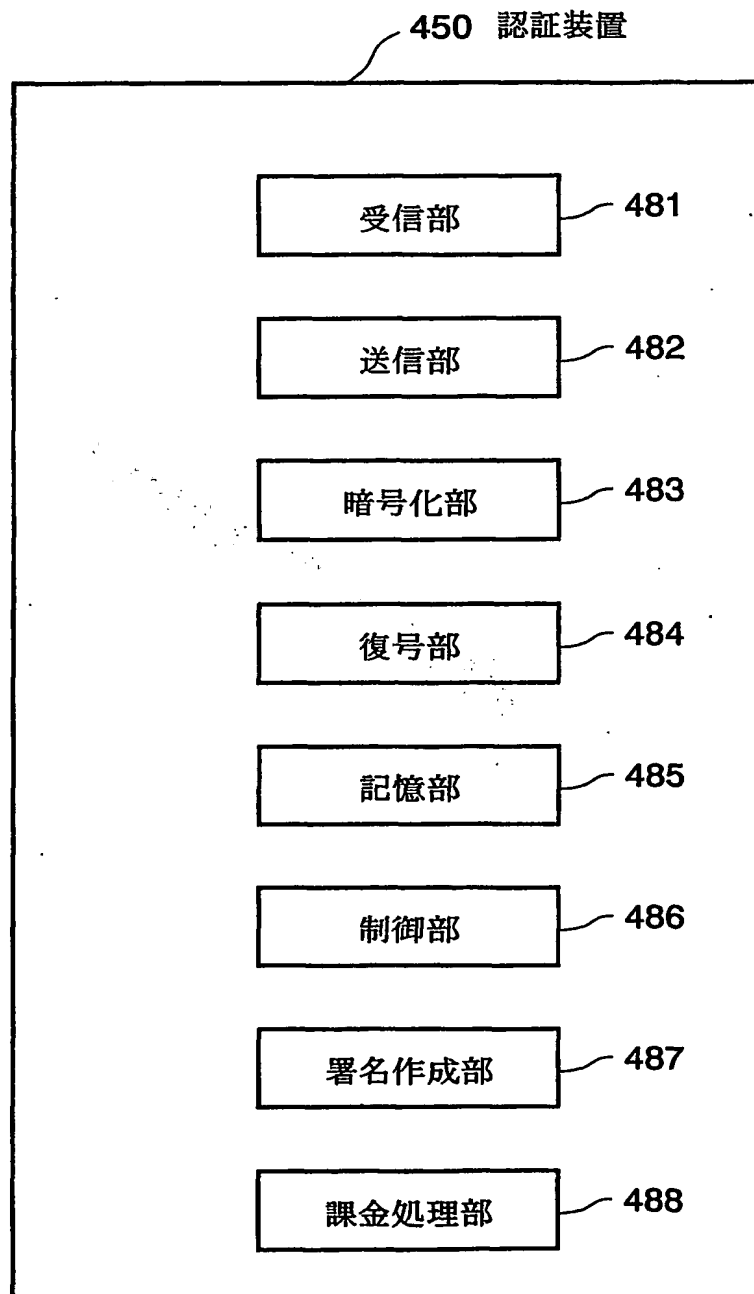
This Page Blank (USP 14)

FIG.32



This Page Blank (uspto)

FIG.33

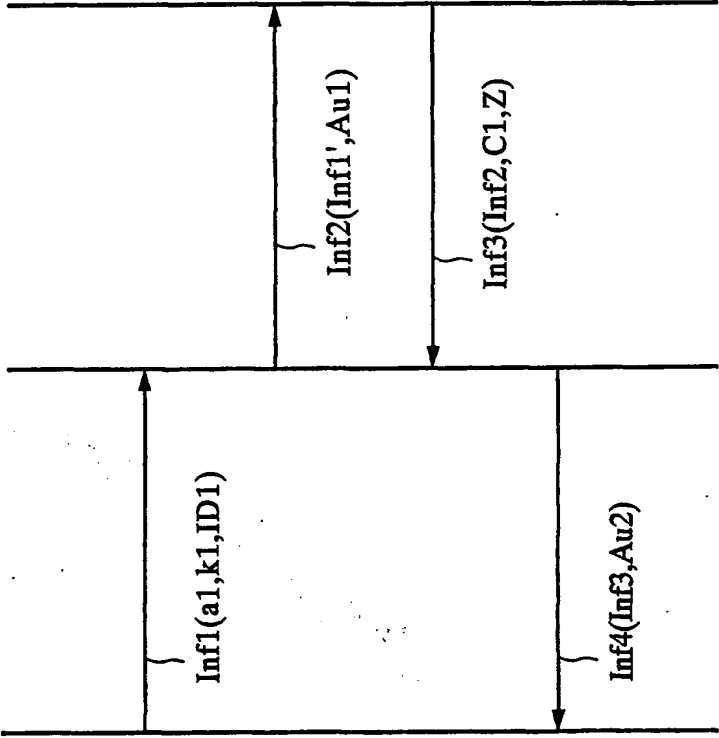


This Page Blank (USP10)

発注者
端末装置411

認証装置
450

受注者
端末装置415



ST41

ST42

ST43

ST44

FIG.34A

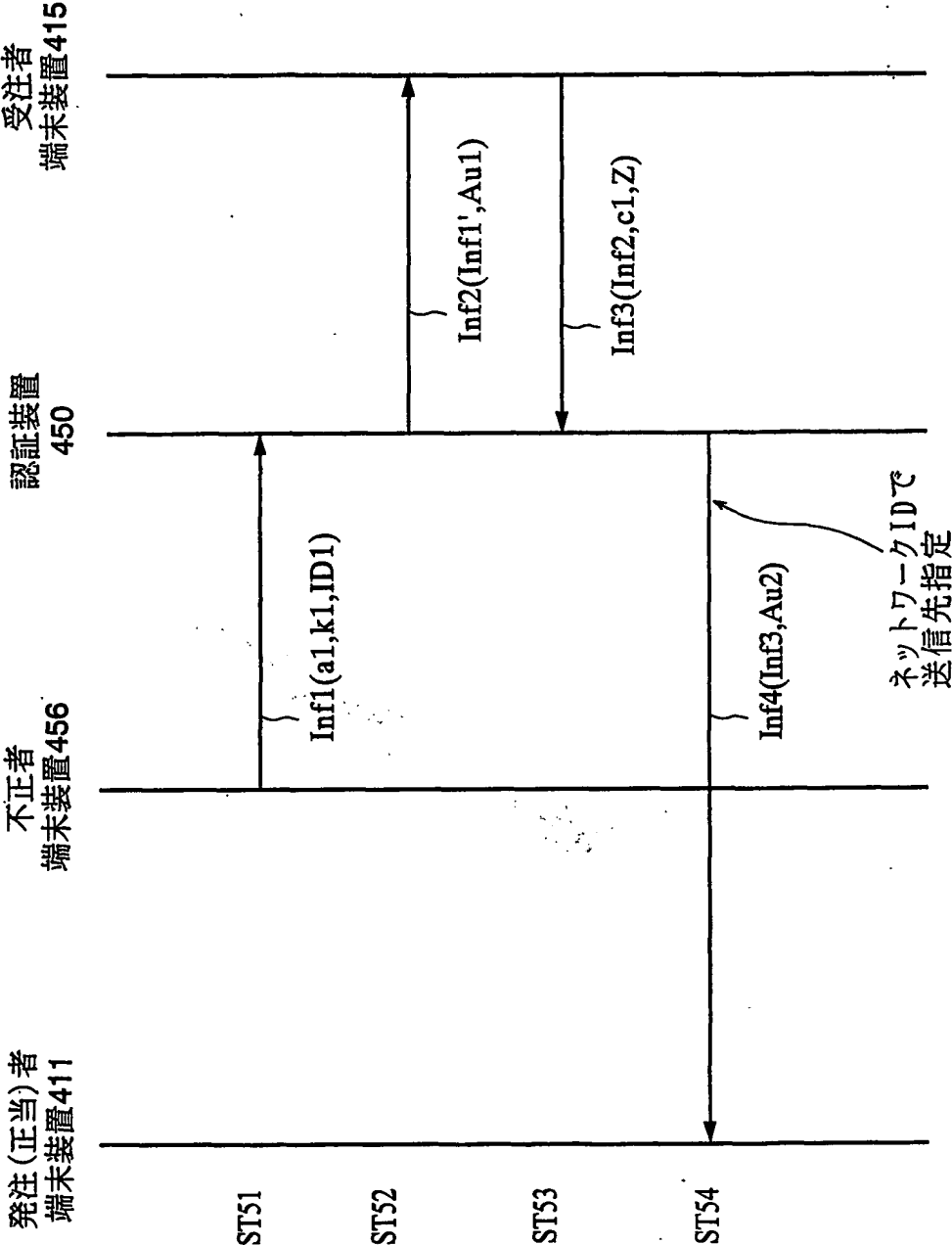
FIG.34B

FIG.34C

FIG.34D

Inf1'=Inf1からk1およびID1を削除した情報

This Page Blank (uspio)



Inf1'=Inf1からk1およびID1を削除した情報

FIG.35A

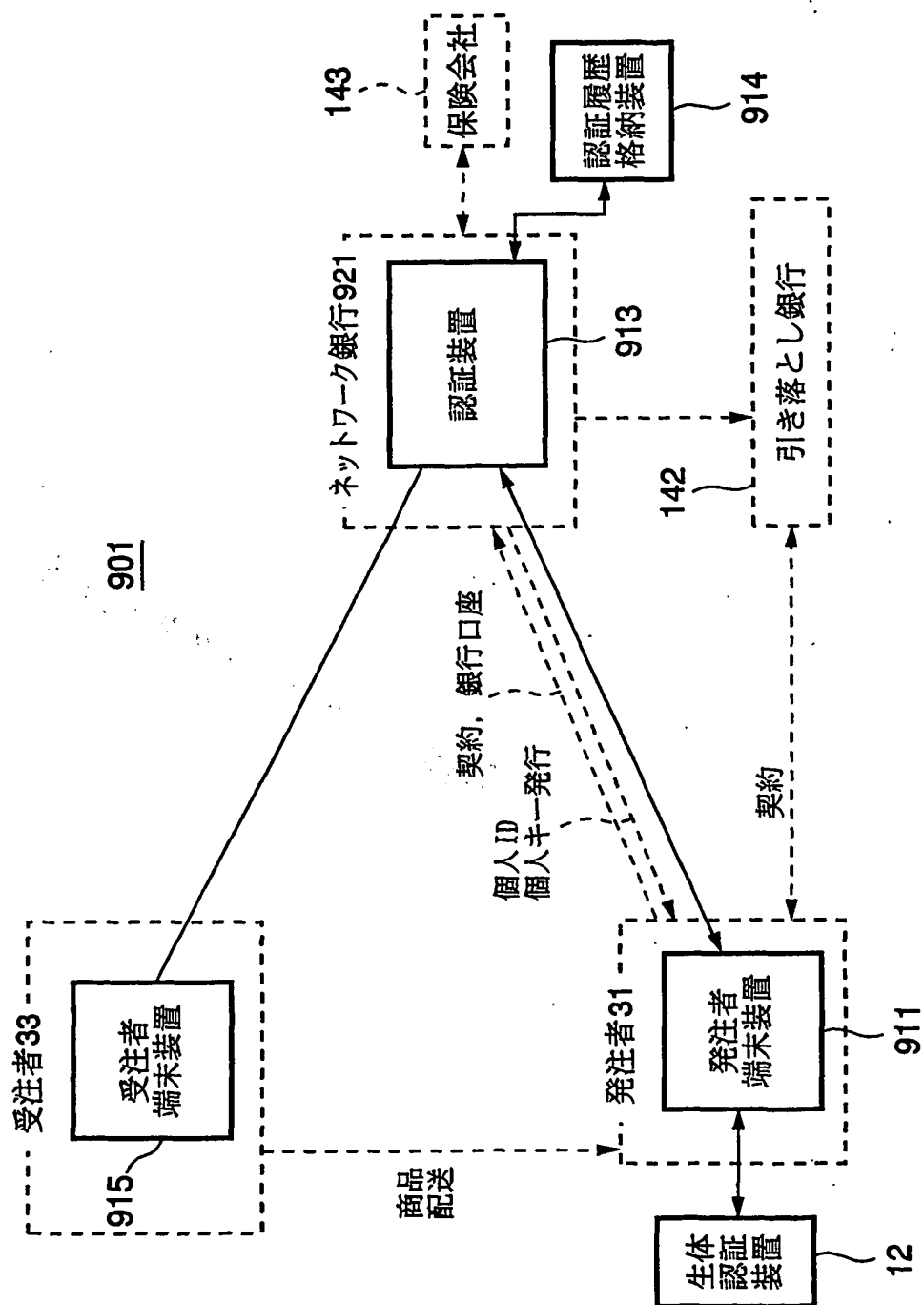
FIG.35B

FIG.35C

FIG.35D

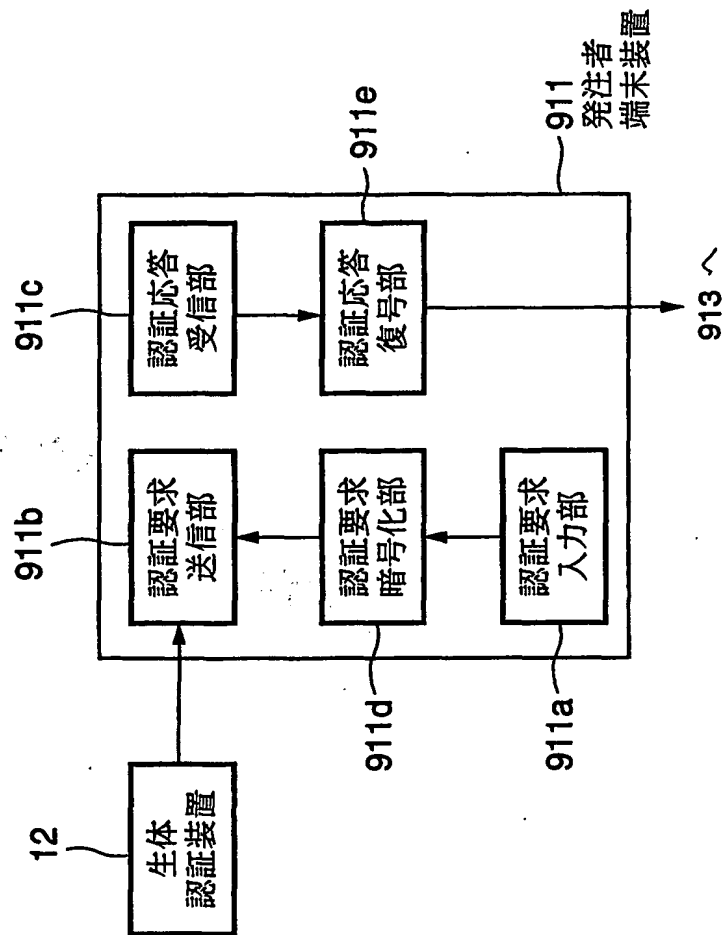
This Page Blank (usp10)

FIG.36



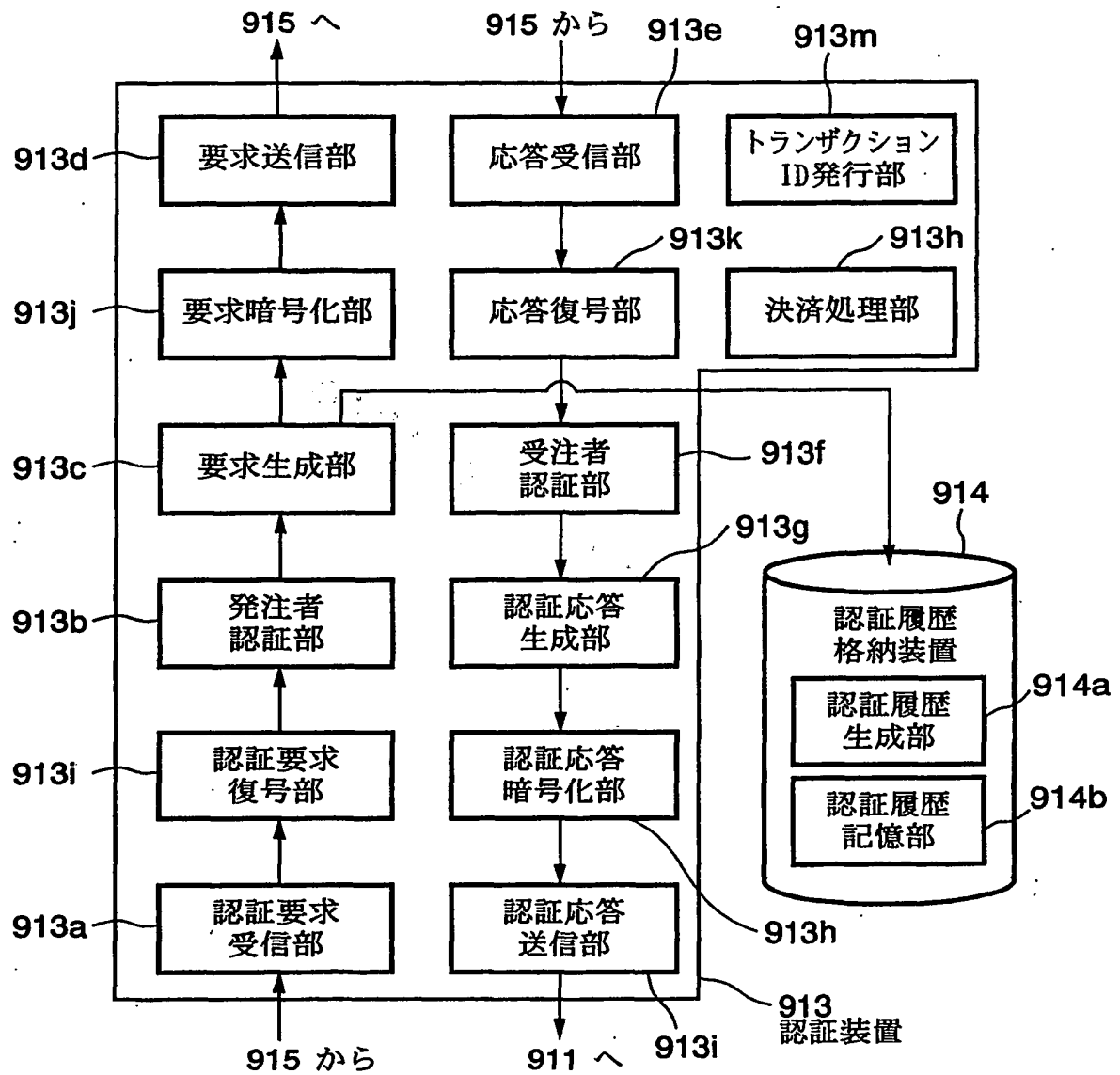
This Page Blank (USP 10)

FIG.37



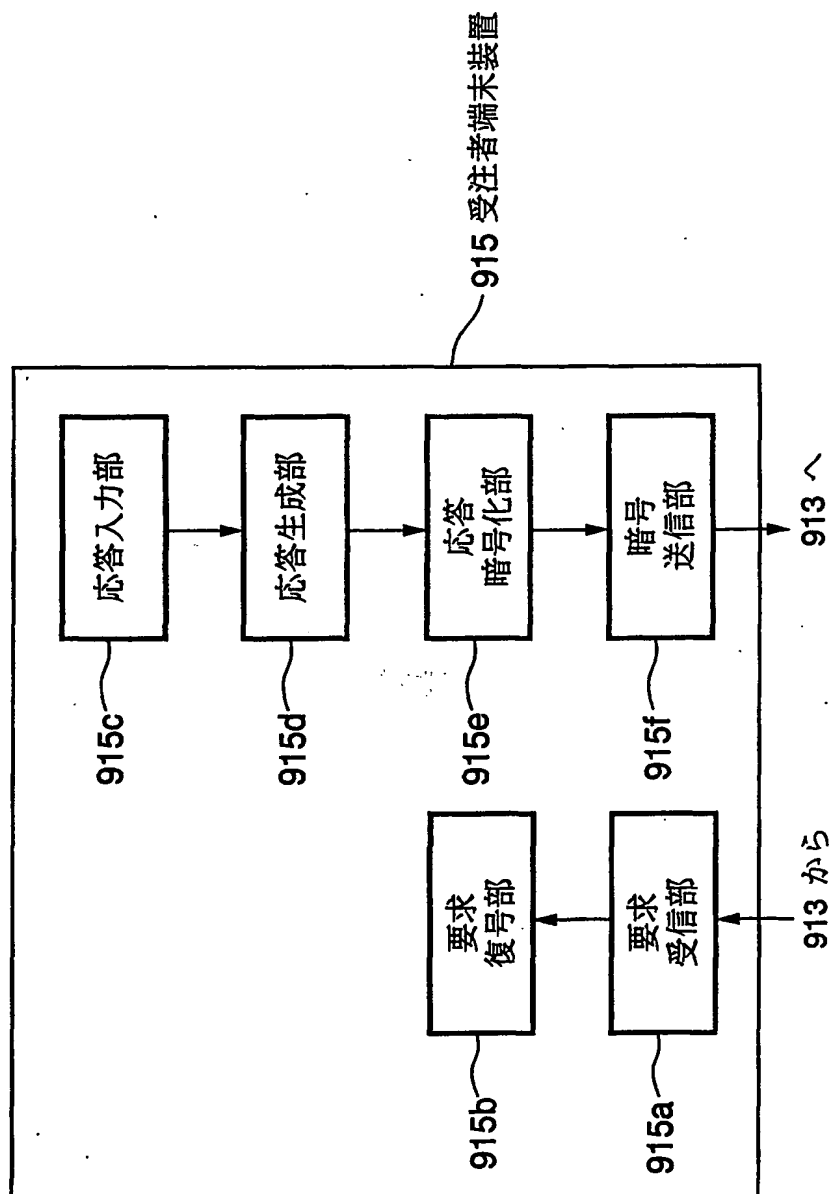
This Page Blank (usp10)

FIG.38



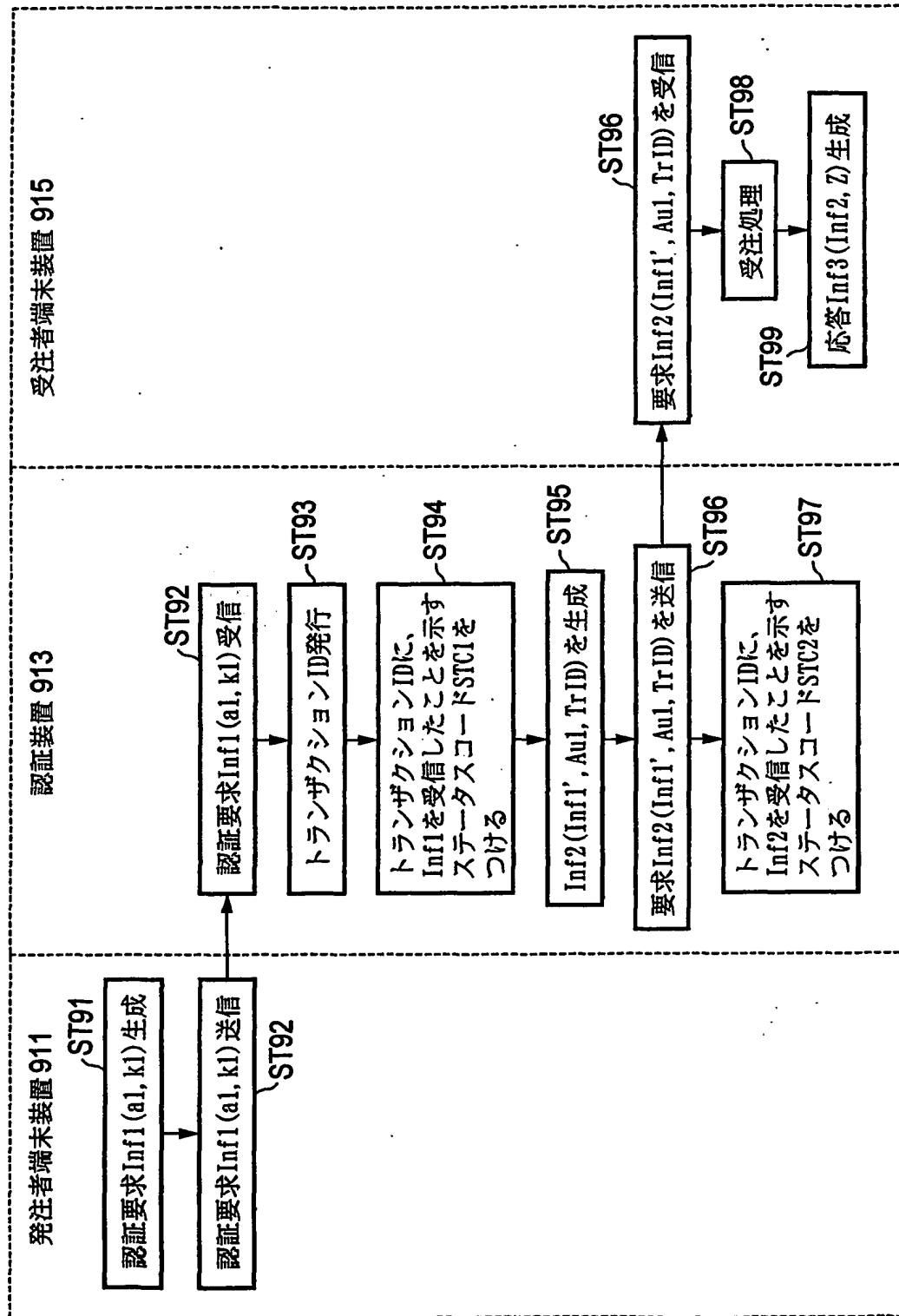
This Page Blank (uspio)

FIG.39



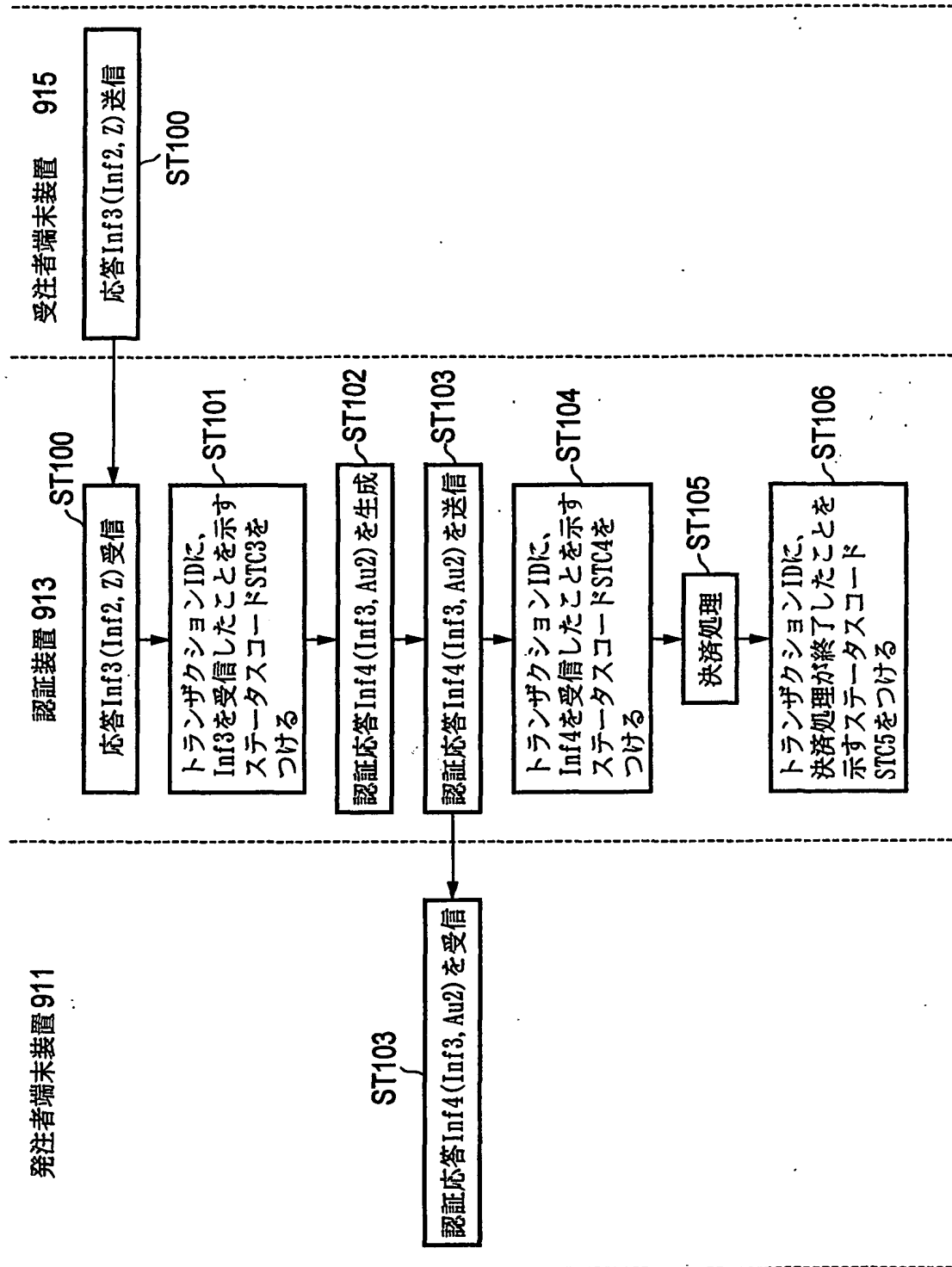
This Page Blank (uspto)

FIG.40



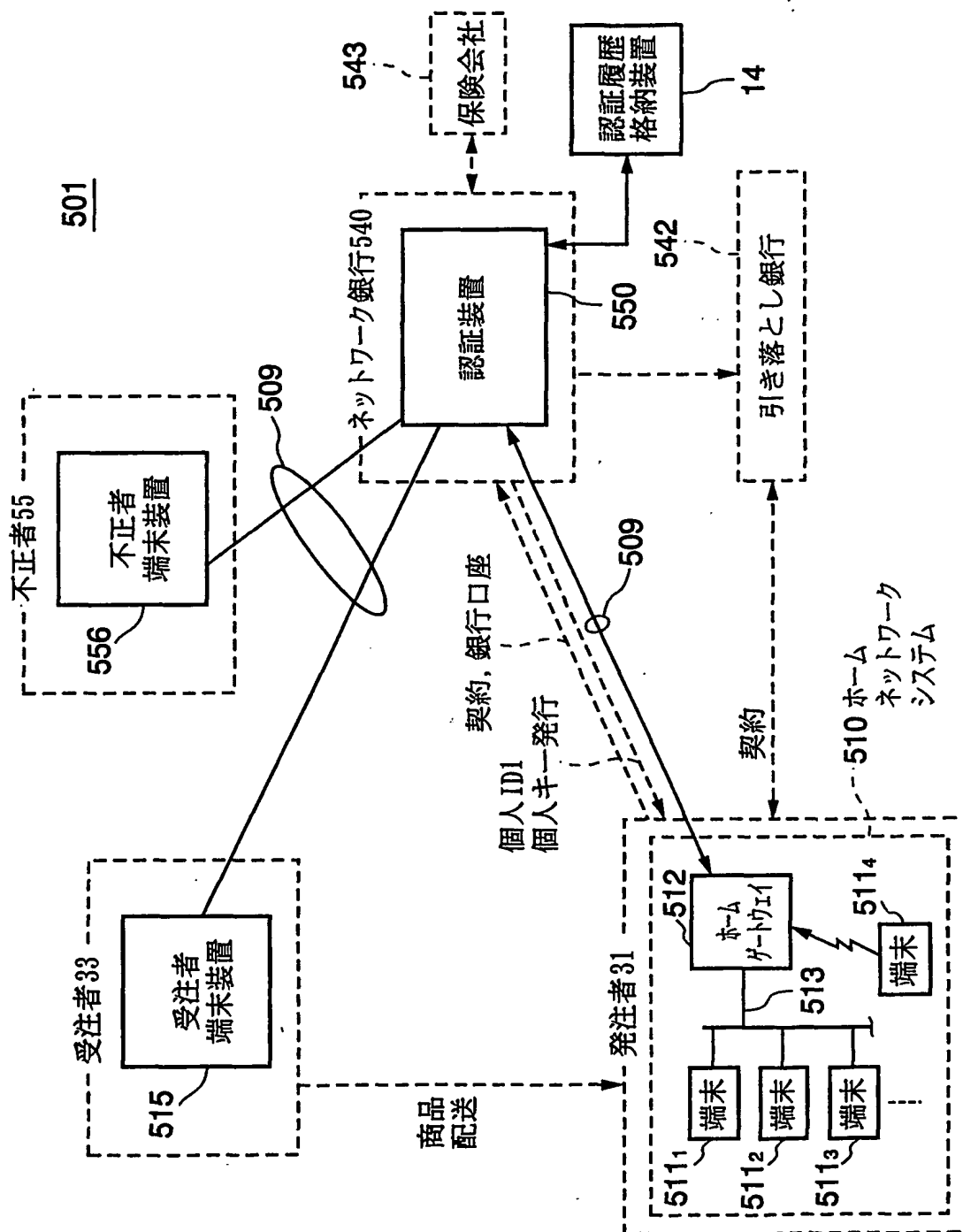
This Page Blank (Copy)

FIG. 41



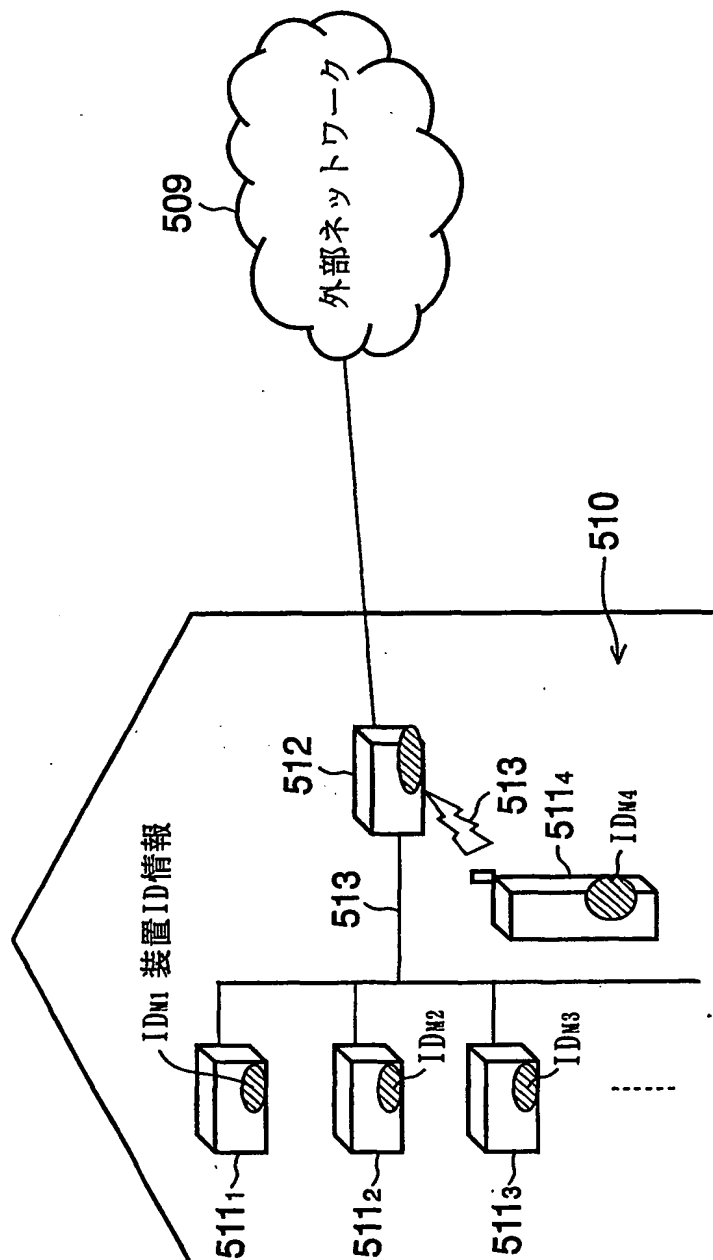
This Page Blank (uspio)

FIG. 42



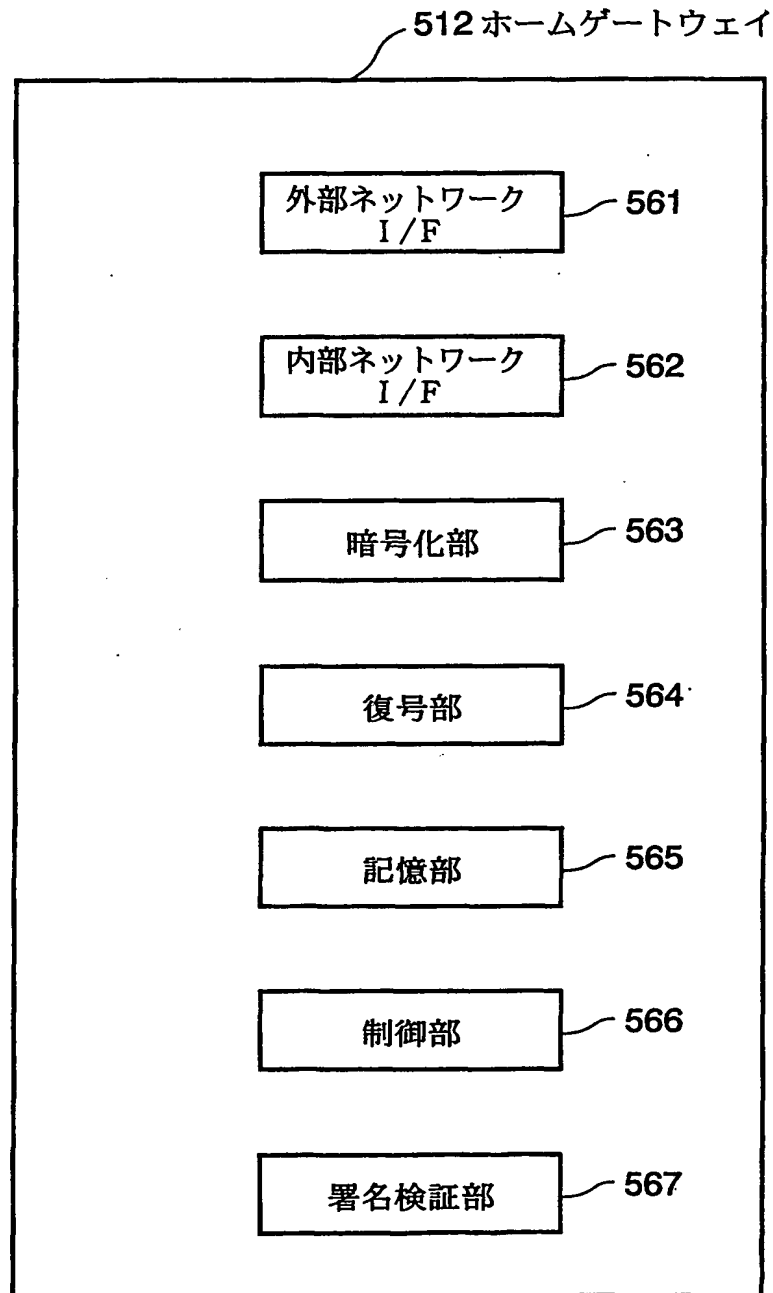
This Page Blank (uspto)

FIG.43



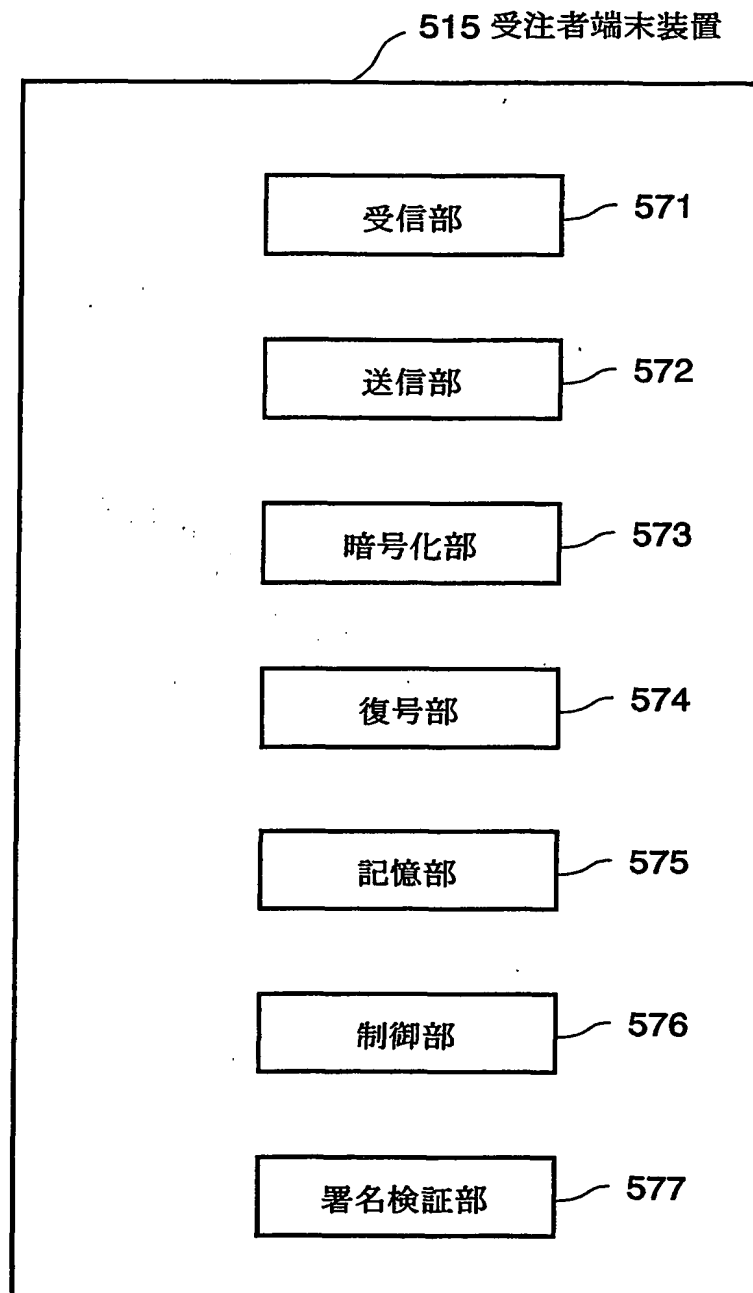
This Page Blank (USP10)

FIG.44



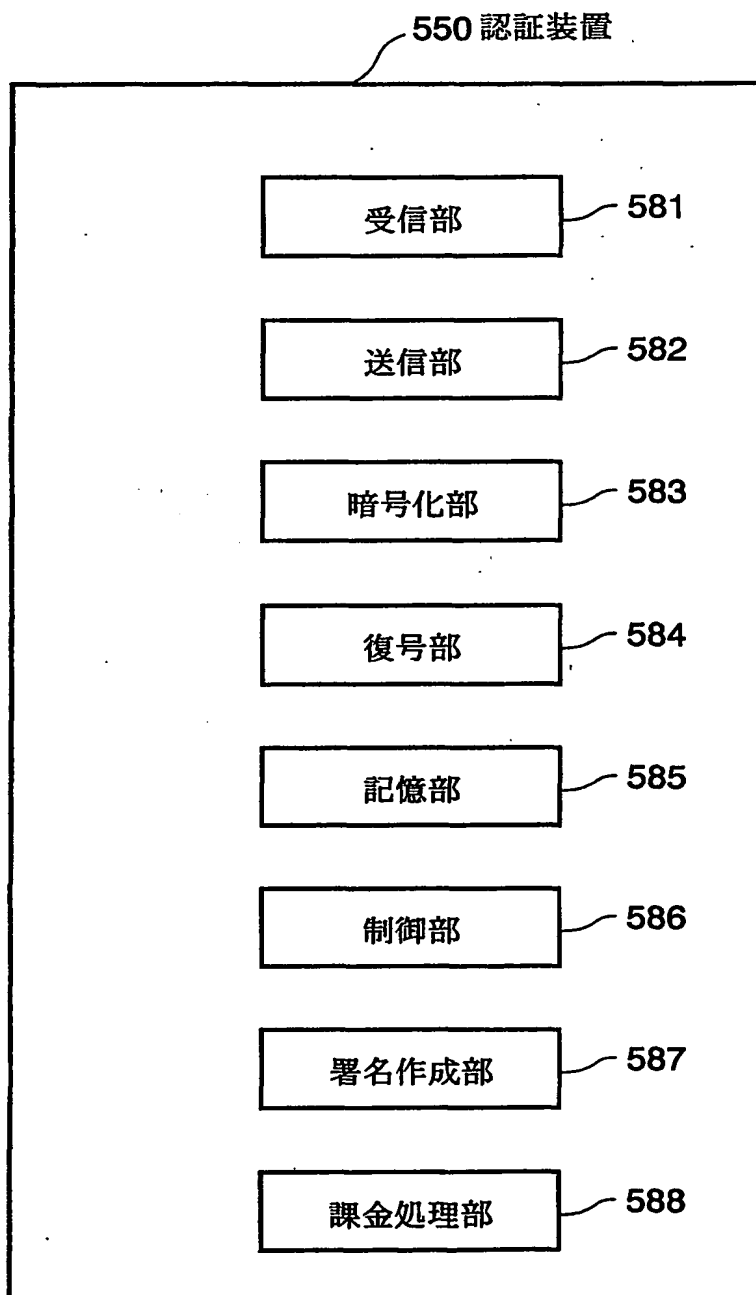
This Page Blank (USP10)

FIG.45



This Page Blank (uspis)

FIG.46



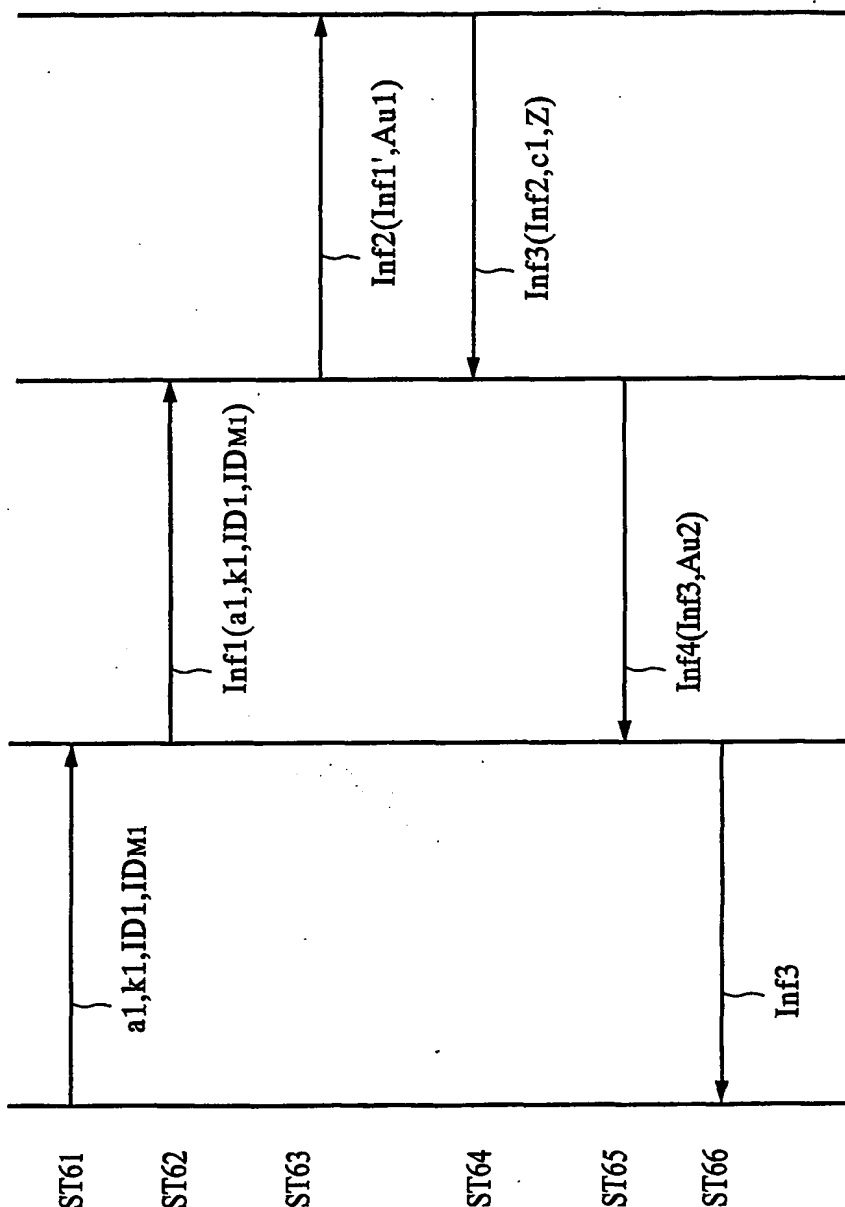
This Page Blank (uspto)

受注者
端末装置 515

認証装置
550

ホーム
ゲートウェイ 512

端末装置 511₁



Inf1'=Inf1からk1およびID1を削除した情報

FIG.47A

FIG.47B

FIG.47C

FIG.47D

FIG.47E

FIG.47F

This Page Blank (uspio)

不正者 発注者 ホーム 認証装置 受注者
端末装置556 端末装置511₁ ゲートウェイ512 550 端末装置515

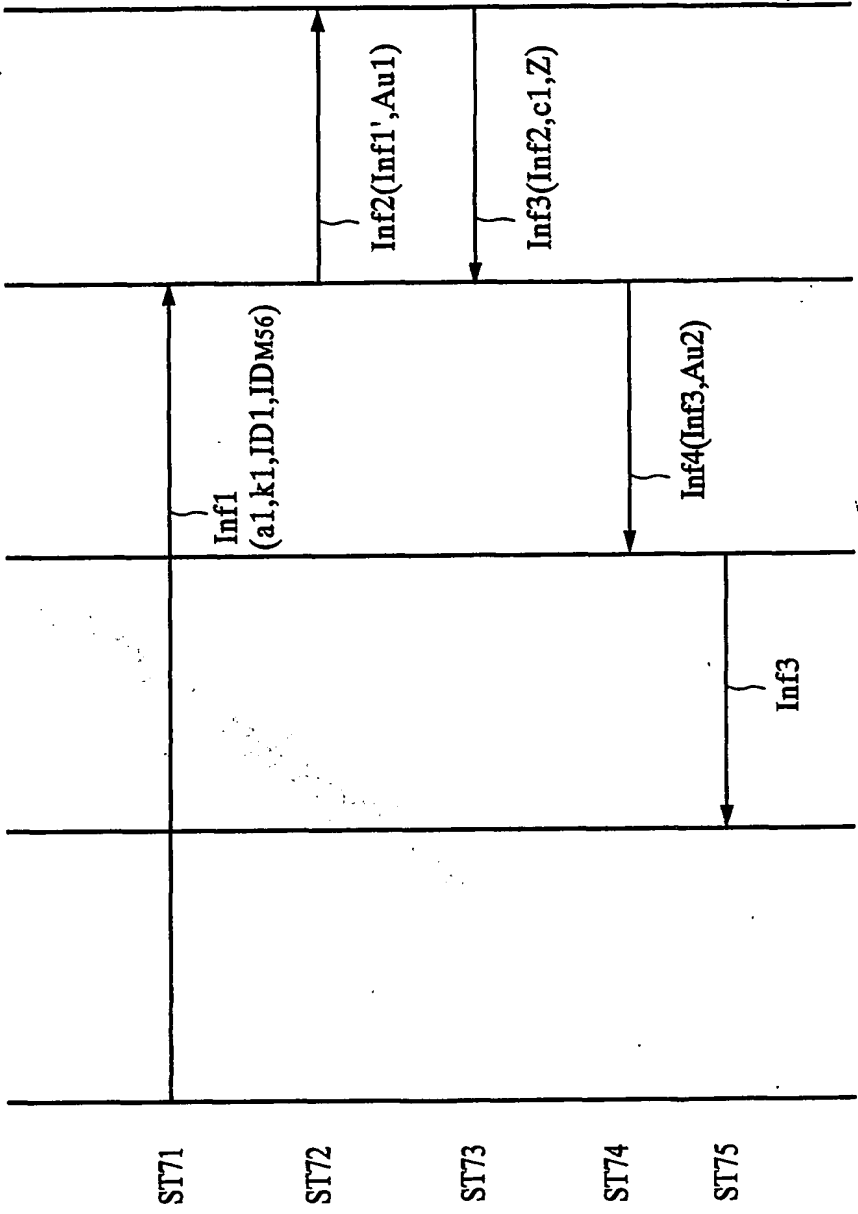


FIG.48A

FIG.48B

FIG.48C

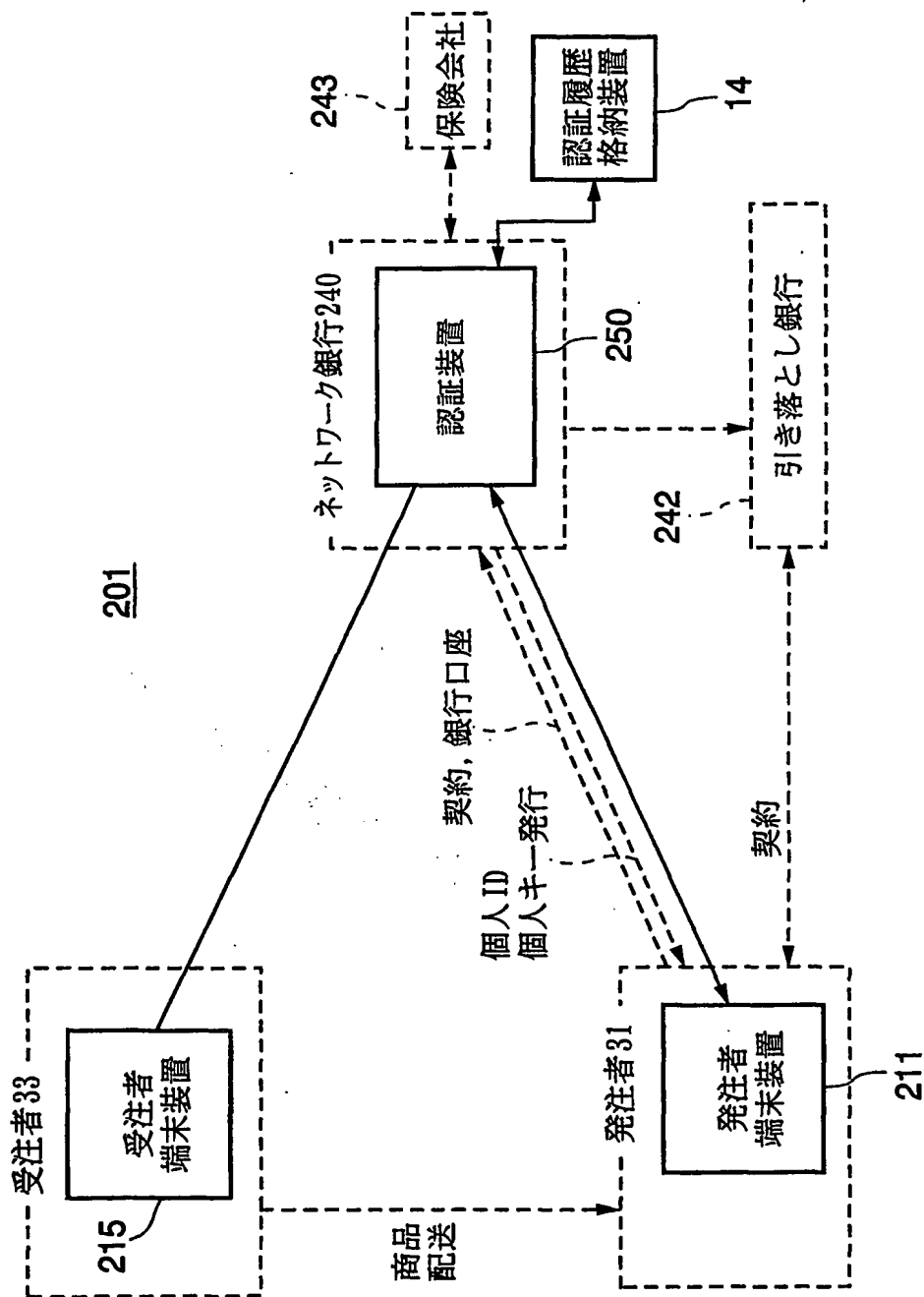
FIG.48D

FIG.48E

Inf1'=Inf1からk1およびID1を削除した情報

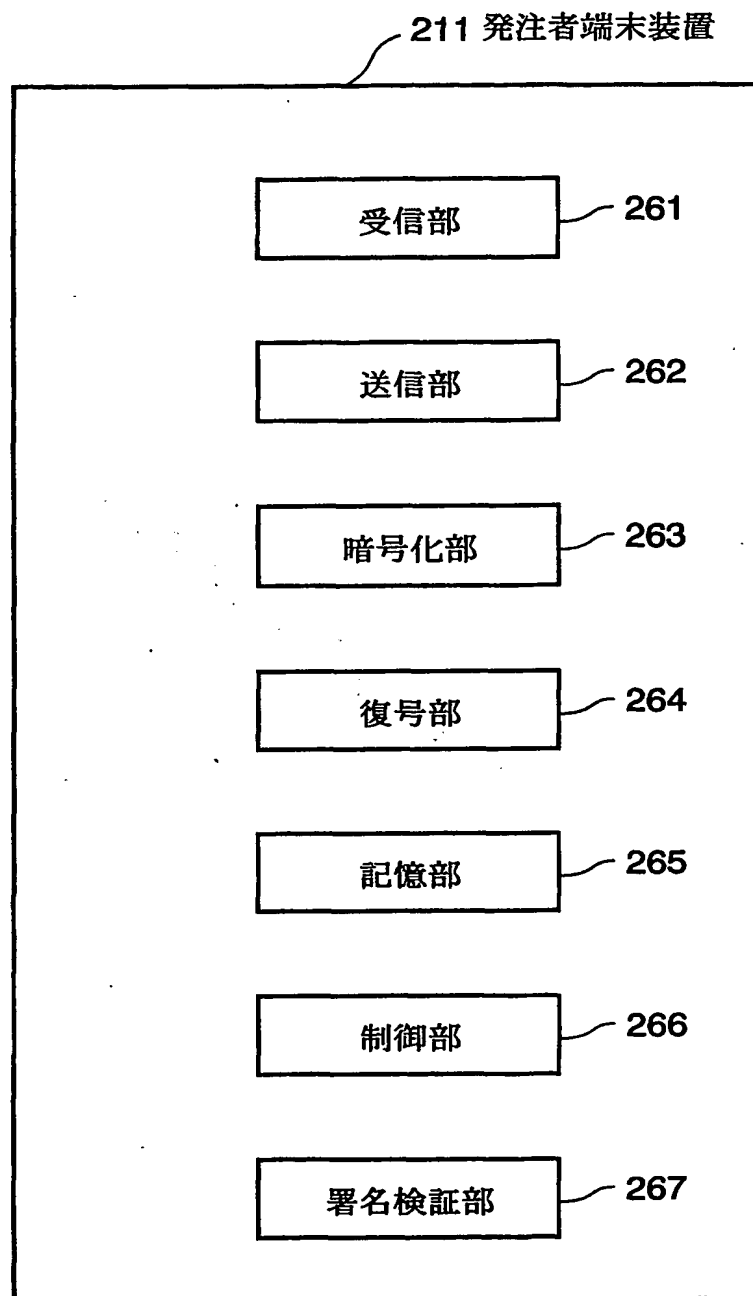
This Page Blank (uspto)

FIG.49



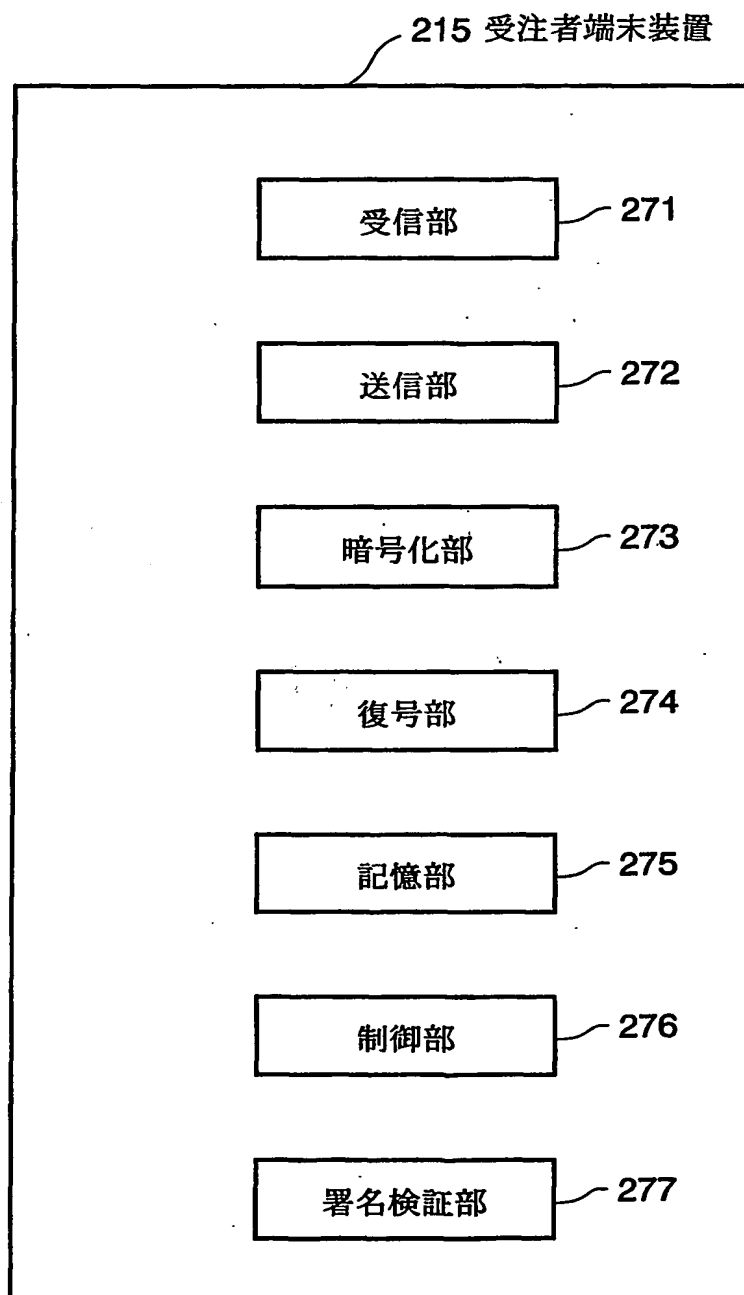
This Page Blank (uspio)

FIG.50



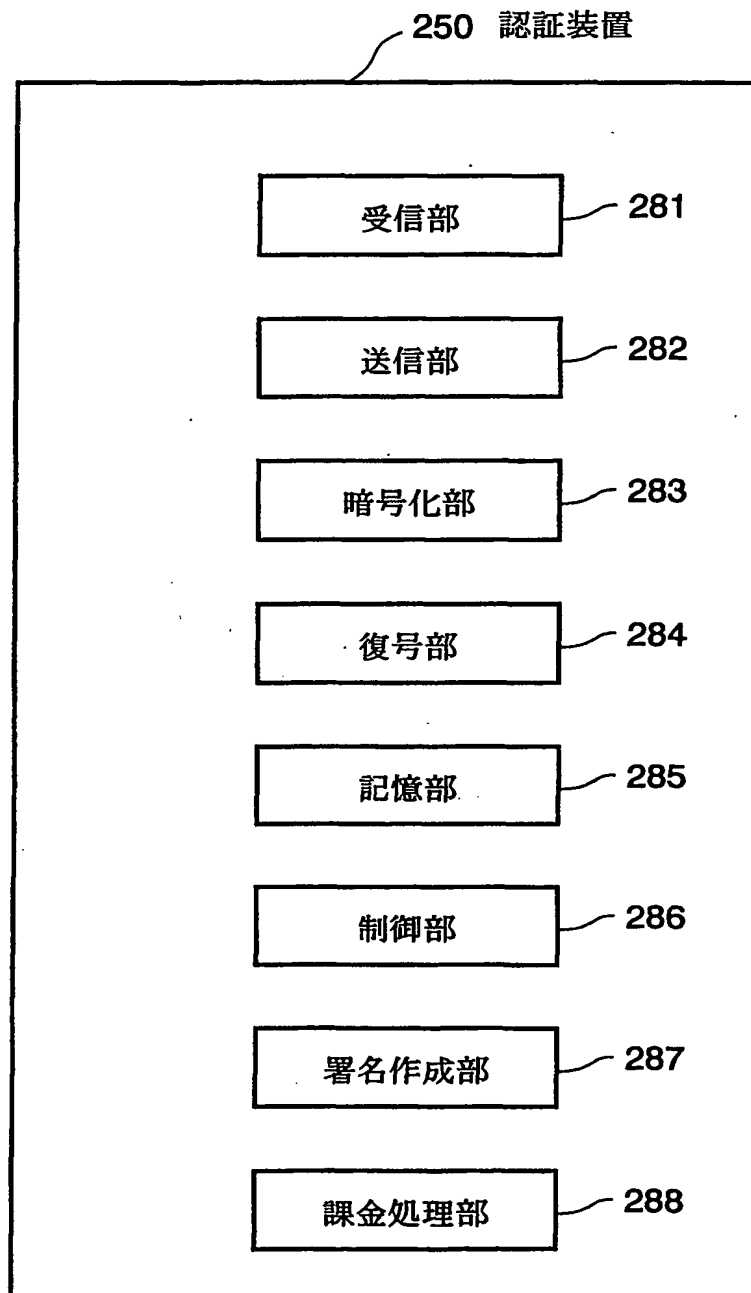
This Page Blank (uspto)

FIG.51



This Page Blank (uspto)

FIG.52

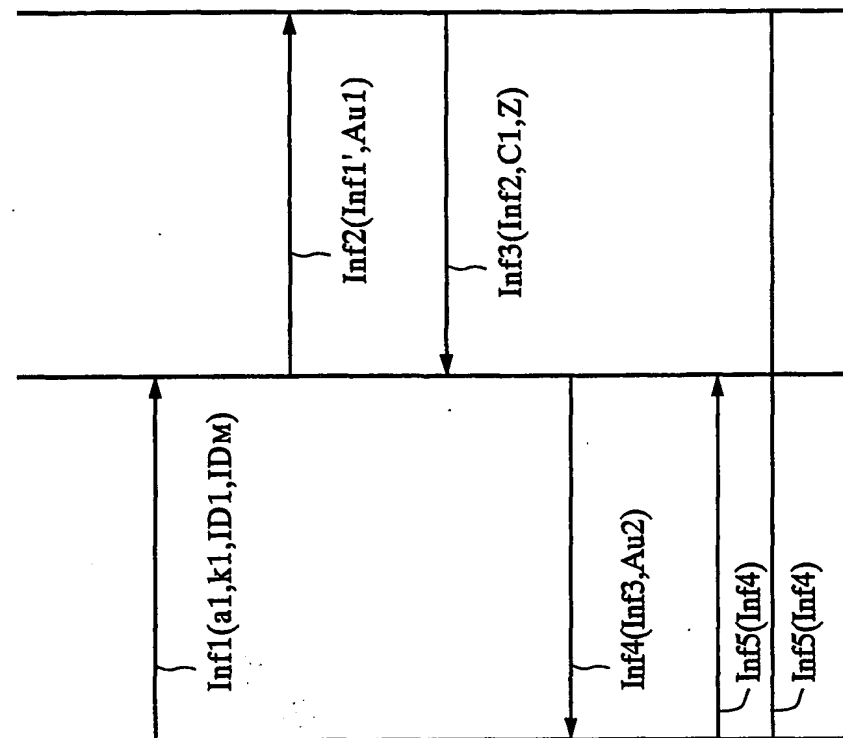


This Page Blank (uspto)

発注者
端末装置211

認証装置
250

受注者
端末装置215



Inf1'=Inf1からk1およびID1を削除した情報

FIG.53A ST21

FIG.53B ST22

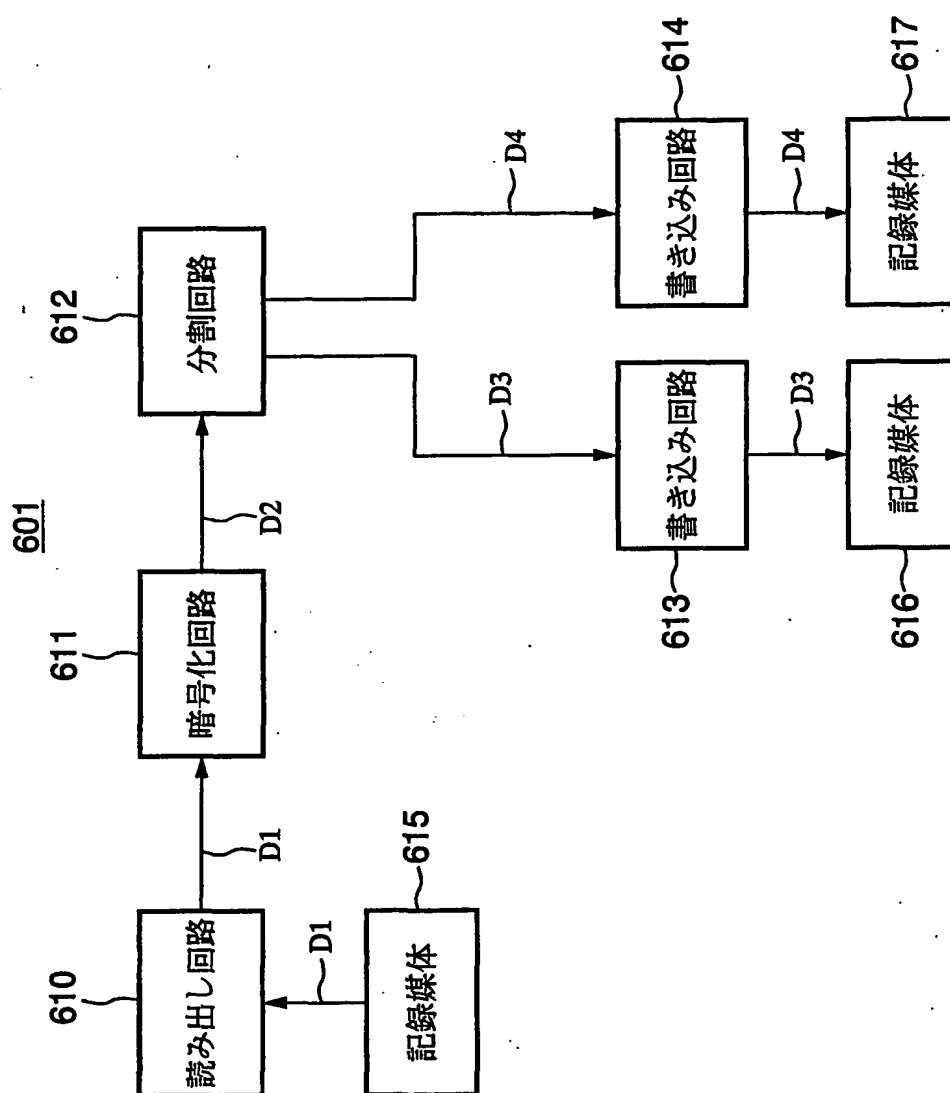
FIG.53C ST23

FIG.53D ST12

FIG.53E ST25

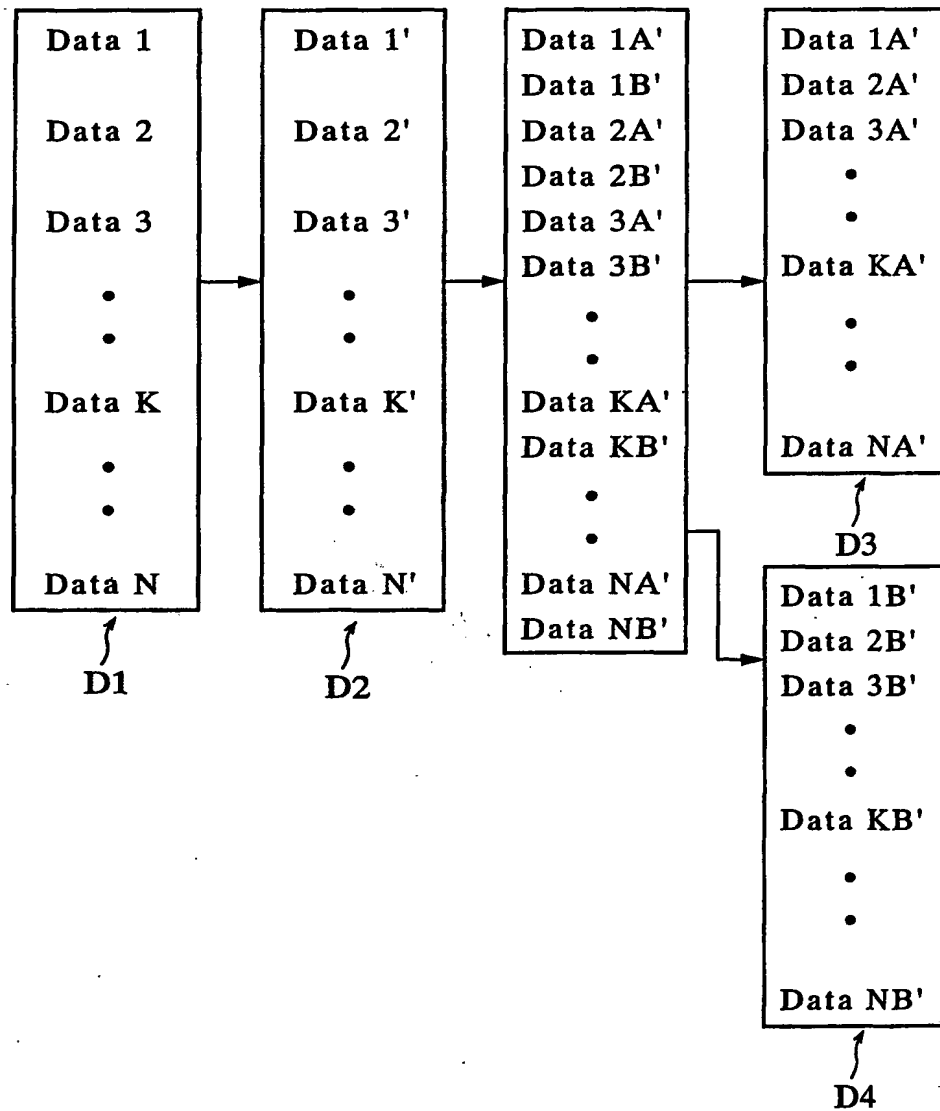
This Page Blank (uspio)

FIG. 54



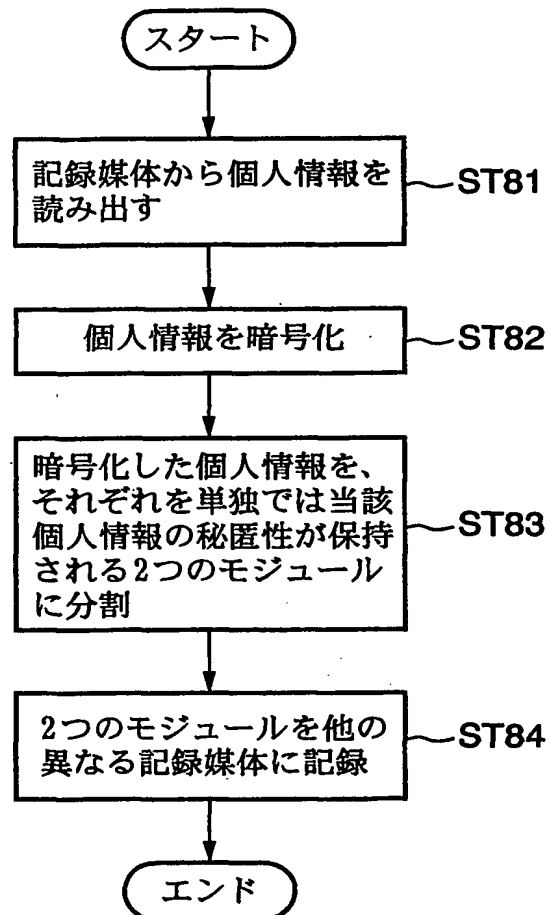
This Page Blank (unpaved)

FIG.55



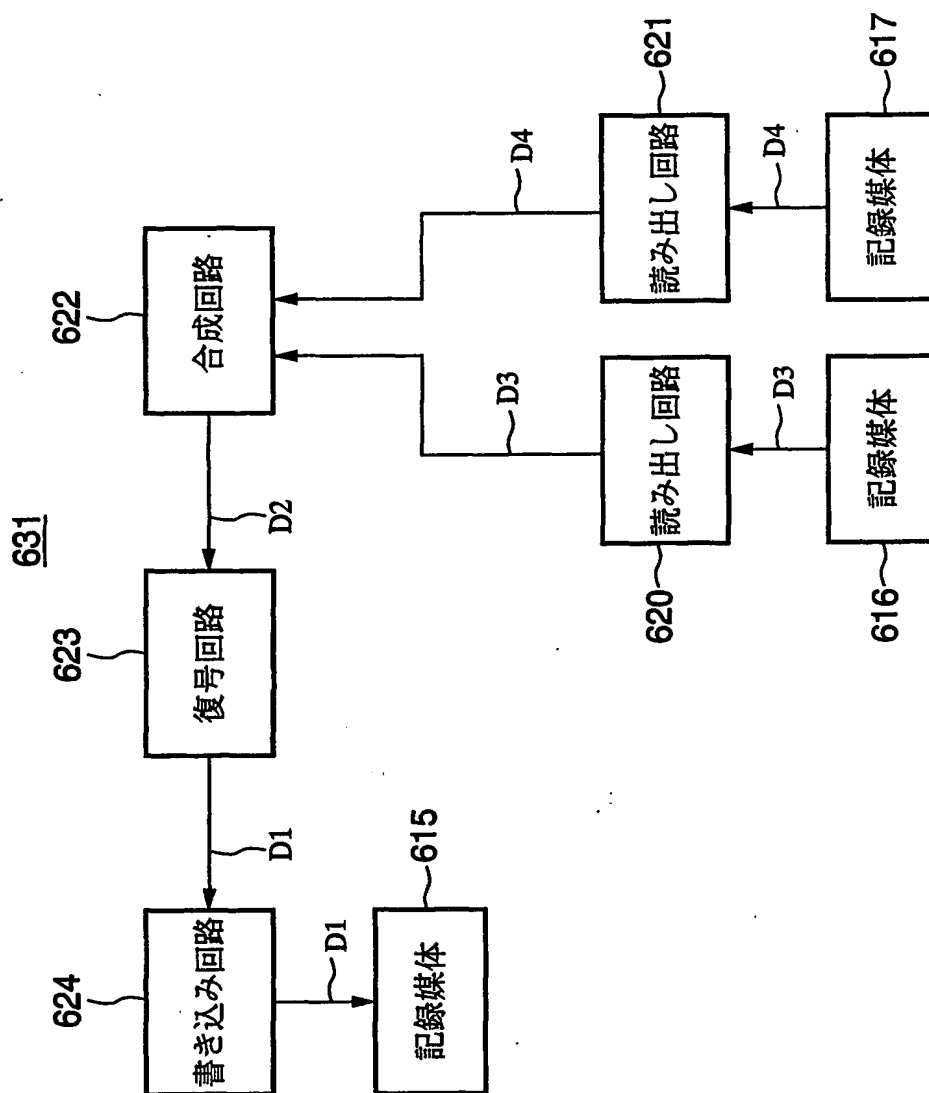
This Page Blank (using)

FIG.56



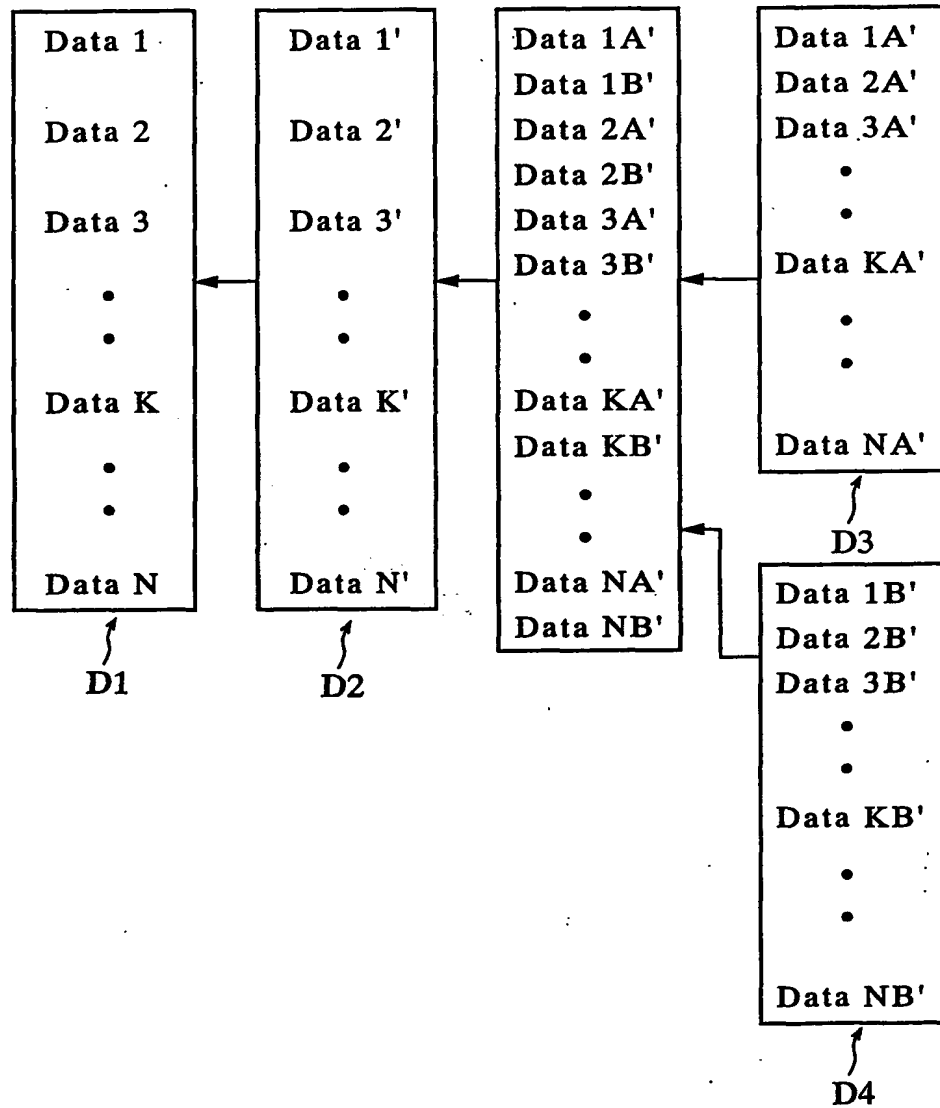
This Page Blank (USP 121)

FIG. 57



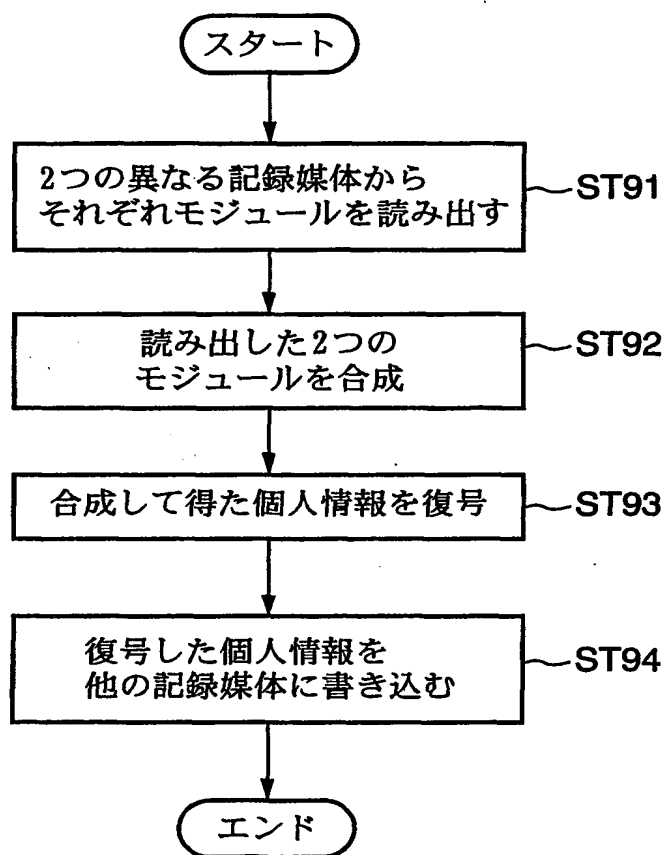
This Page Blank (uspic)

FIG.58



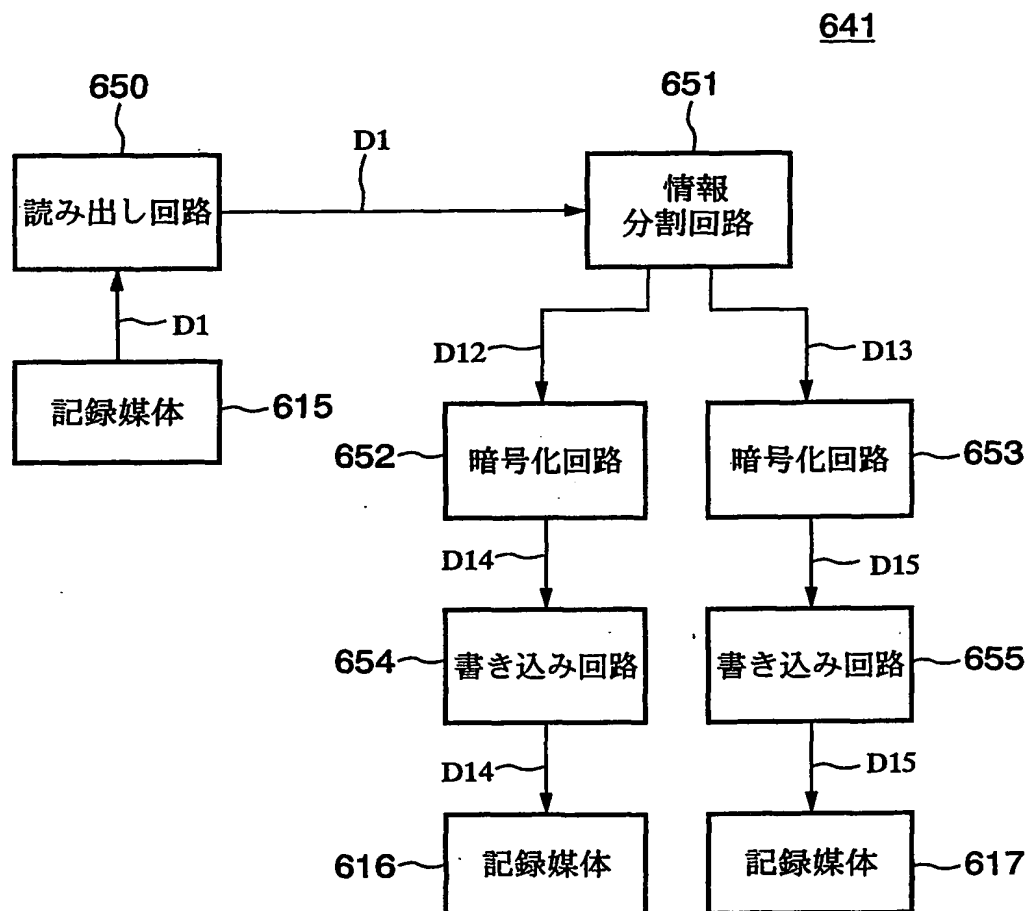
This Page Blank (USP 119)

FIG.59



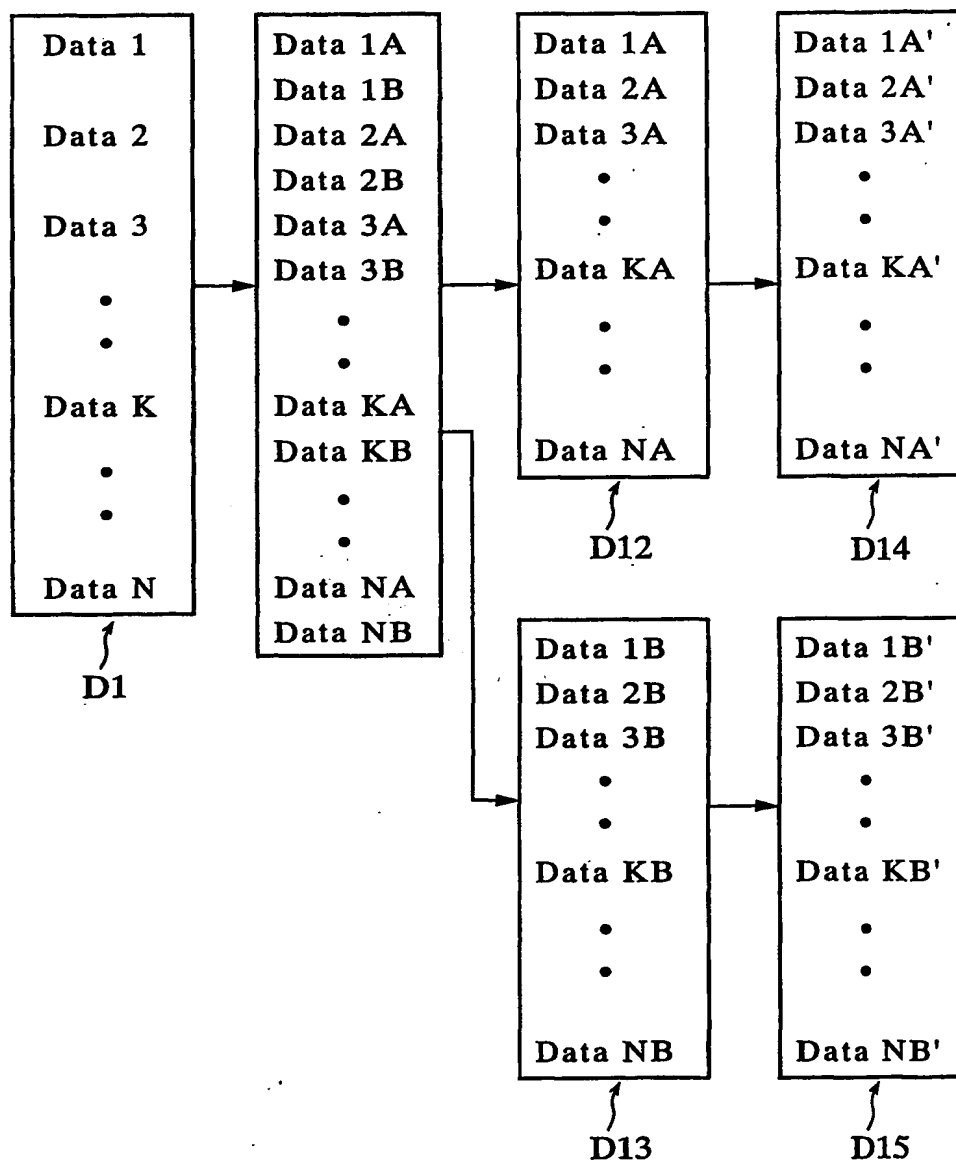
This Page Blank (uspto)

FIG.60



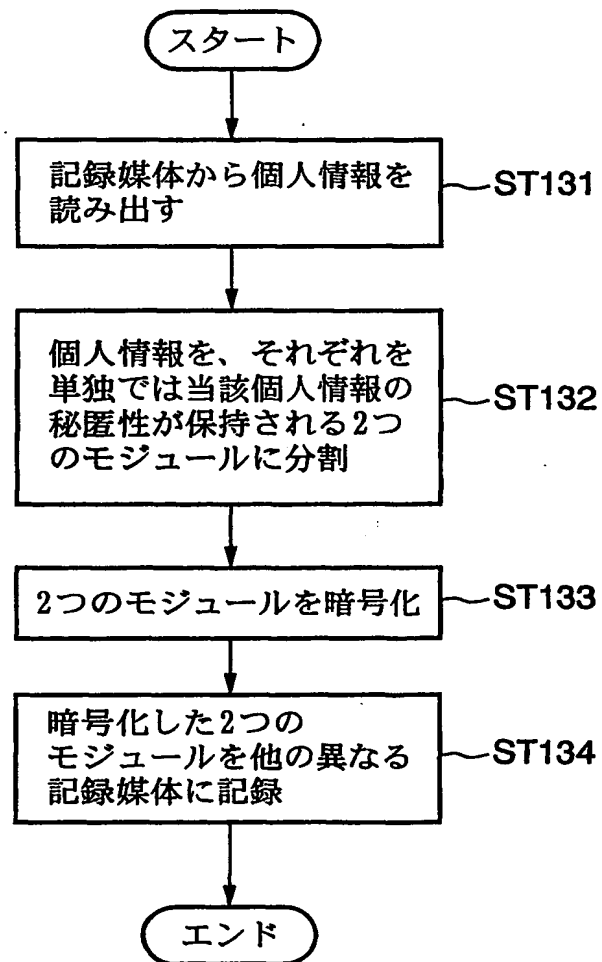
This Page Blank (uspto)

FIG.61



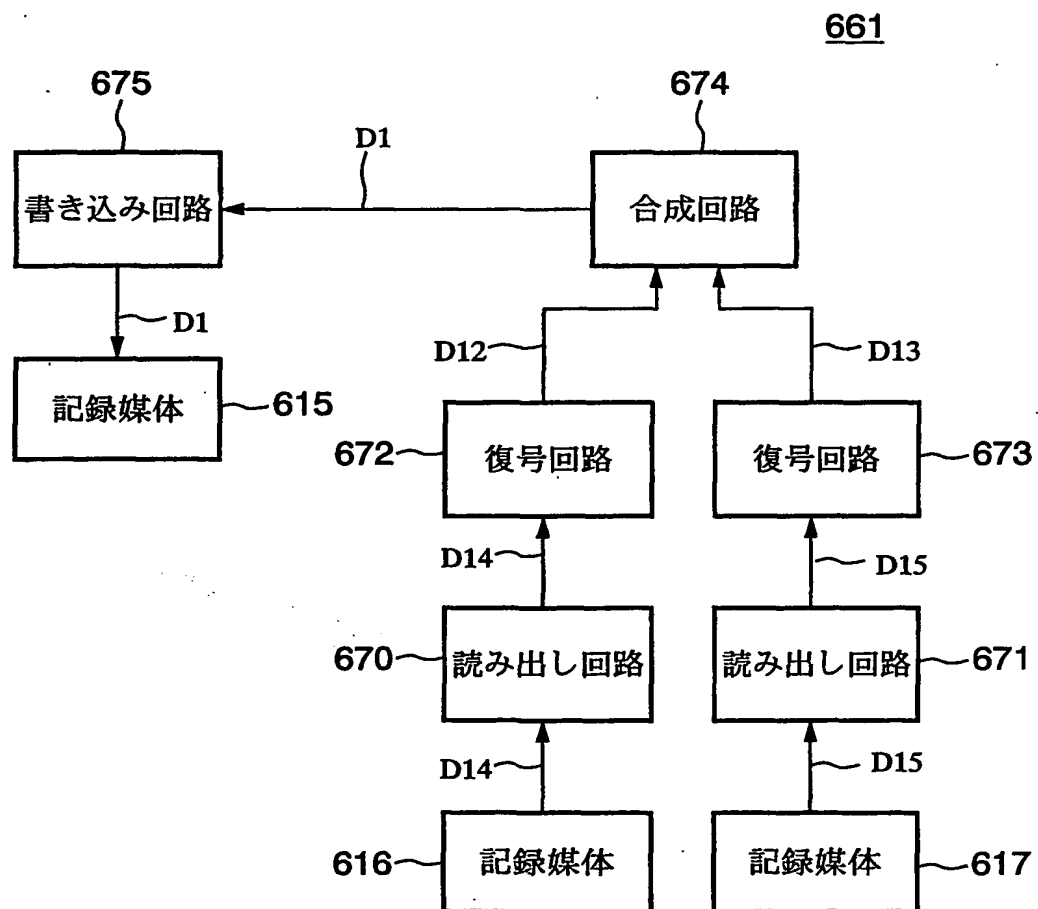
This Page Blank (uspto)

FIG.62



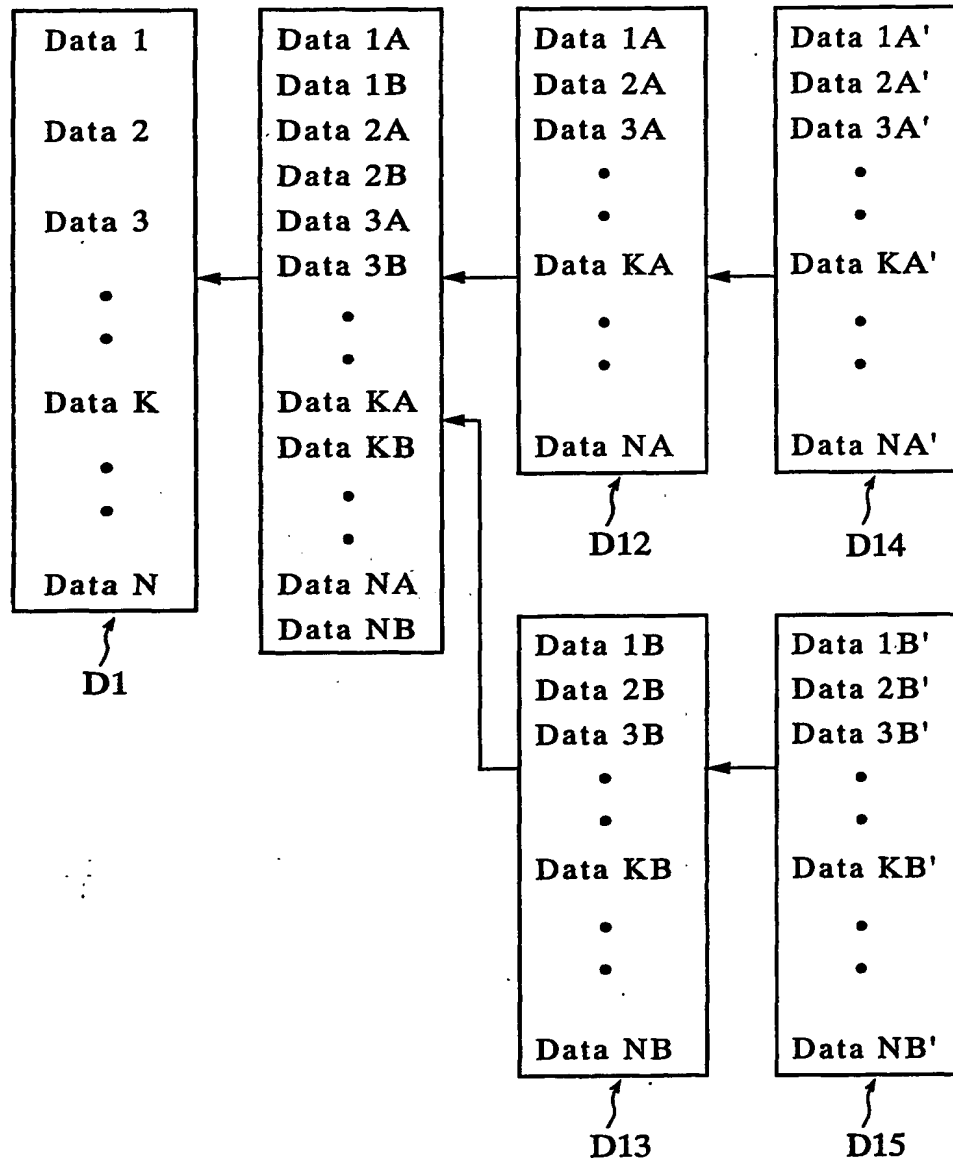
This Page Blank (USC 1)

FIG.63



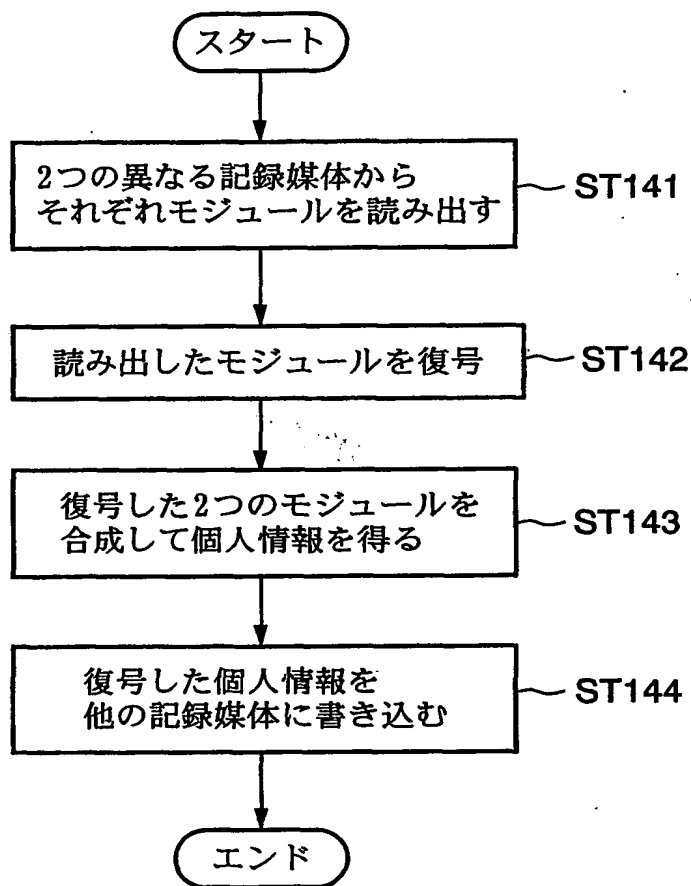
This Page Blank (U.S. 1)

FIG.64



This Page Blank (10/9/01)

FIG.65



This Page Blank (USP 114)

符号リスト

1 …トランザクション認証システム

1 1 …発注者端末装置

1 1 a …認証要求入力部

1 1 b …認証要求送信部

1 1 c …認証応答受信部

1 1 d …認証要求暗号化部

1 1 e …認証応答復号部

1 2 …生体認証装置

1 3 …認証装置

1 3 a …認証要求受信部

1 3 b …発注者認証部

1 3 c …要求生成部

1 3 d …要求送信部

1 3 e …応答受信部

1 3 f …受注者認証部

1 3 g …認証応答生成部

1 3 h …認証応答暗号化部

1 3 i …認証応答送信部

1 3 j …要求暗号化部

1 3 k …応答復号部

1 3 l …認証要求復号部

1 4 …認証履歴格納装置

1 5 …受注者端末装置

1 5 a …認証要求受信部

This Page Blank (used)

1 5 b …要求復号部

1 5 c …応答入力部

1 5 d …応答生成部

1 5 e …応答暗号化部

1 5 f …応答送信部

1 0 1 …トランザクション認証システム

1 0 1 1 …発注者端末装置

1 0 1 1 a …認証要求入力部

1 0 1 1 b …認証要求送信部

1 0 1 1 c …認証応答受信部

1 0 1 d …認証要求暗号化部

1 0 1 e …認証応答復号部

1 2 …生体認証装置

1 1 3 …認証装置

1 1 3 a …認証要求受信部

1 1 3 b …発注者認証部

1 1 3 c …要求生成部

1 1 3 d …要求送信部

1 1 3 e …応答受信部

1 1 3 f …受注者認証部

1 1 3 g …認証応答生成部

1 1 3 h …認証応答暗号化部

1 1 3 i …認証応答送信部

1 1 3 j …要求暗号化部

1 1 3 k …応答復号部

This Page Blank (uspto)

- 1 1 3 1 … 認証要求復号部
- 1 4 … 認証履歴格納装置
- 1 5 … 受注者端末装置
- 1 1 5 a … 認証要求受信部
- 1 1 5 b … 要求復号部
- 1 1 5 c … 応答入力部
- 1 1 5 d … 応答生成部
- 1 1 5 e … 応答暗号化部
- 1 1 5 f … 応答送信部

- 2 0 1 … トランザクション認証システム
- 2 1 1 … 発注者端末装置
- 2 1 5 … 受注者端末装置
- 3 1 … 発注者
- 3 3 … 受注者
- 2 4 0 … ネットワーク銀行
- 2 5 0 … 認証装置
- 2 6 1, 2 7 1, 2 8 1 … 受信部
- 2 6 2, 2 7 2, 2 8 2 … 送信部
- 2 6 3, 2 7 3, 2 8 3 … 暗号化部
- 2 6 4, 2 7 4, 2 8 4 … 復号部
- 2 6 5, 2 7 5, 2 8 5 … 記憶部
- 2 6 6, 2 7 6, 2 8 6 … 制御部
- 2 6 7, 2 7 7 … 署名検証部
- 2 8 7 … 署名作成部
- 2 8 8 … 課金処理部

This Page Blank (unp'd)

a 1 …発注情報

k 1 …発注者 3 1 の個人キー情報 k 1

I D 1 …発注者 3 1 の個人 I D 情報

I D_M …装置 I D 情報

A u 1, A u 2 …認証装置の署名情報

Z …受注者を特定する情報

I n f 1 …認証要求

I n f 4 …認証応答

3 0 1 …トランザクション認証システム

3 1 1 …発注者端末装置

3 1 5 …受注者端末装置

3 4 0, 3 4 1 …ネットワーク銀行

3 5 0, 3 5 1 …認証装置

3 6 1, 3 7 1, 3 8 1, 3 9 1 …受信部

3 6 2, 3 7 2, 3 8 2, 3 9 2 …送信部

3 6 3, 3 7 3, 3 8 3, 3 9 3 …暗号化部

3 6 4, 3 7 4, 3 8 4, 3 9 4 …復号部

3 6 5, 3 7 5, 3 8 5, 3 9 5 …記憶部

3 6 6, 3 7 6, 3 8 6, 3 9 6 …制御部

3 6 7, 3 7 7 …署名検証部

3 8 7, 3 9 7 …署名作成部

3 8 8, 3 9 8 …課金処理部

a 1 …発注情報

k 1 …発注者 3 1 の個人キー情報 k 1

This Page Blank (Unfold)

I D 1 …発注者 3 1 の個人 I D 情報

b 1 …受注者を特定する情報

A u - B …認証装置 3 5 1 の署名情報

A u - A 1 , A u - A 2 …認証装置 3 5 0 の署名情報

Z …受注者を特定する情報

1 3 0 1 …トランザクション認証システム

1 3 1 1 …発注者端末装置

1 3 1 5 …受注者端末装置

1 3 4 0 , 1 3 4 1 …ネットワーク銀行

1 3 5 0 , 1 3 5 1 …認証装置

1 3 6 1 , 1 3 7 1 , 1 3 8 1 , 1 3 9 1 …受信部

1 3 6 2 , 1 3 7 2 , 1 3 8 2 , 1 3 9 2 …送信部

1 3 6 3 , 1 3 7 3 , 1 3 8 3 , 1 3 9 3 …暗号化部

1 3 6 4 , 1 3 7 4 , 1 3 8 4 , 1 3 9 4 …復号部

1 3 6 5 , 1 3 7 5 , 1 3 8 5 , 1 3 9 5 …記憶部

1 3 6 6 , 1 3 7 6 , 1 3 8 6 , 1 3 9 6 …制御部

1 3 6 7 , 1 3 7 7 …署名検証部

1 3 8 7 , 1 3 9 7 …署名作成部

1 3 8 8 , 1 3 9 8 …課金処理部

a 1 …発注情報

k 1 …発注者 3 1 の個人キー情報 k 1

I D 1 …発注者 3 1 の個人 I D 情報

b 1 …受注者を特定する情報

A u - B 1 , A u - B 2 …認証装置 1 3 5 1 の署名情報

This Page Blank (usptol)

A u - A 1, A u - A 2 … 認証装置 1 3 5 0 の署名情報

Z … 受注者を特定する情報の個人キー情報

4 0 1 … トランザクション認証システム

4 1 1 … 発注者端末装置

4 1 5 … 受注者端末装置

4 4 0 … ネットワーク銀行

4 5 0 … 認証装置

4 6 1, 4 7 1, 4 8 1 … 受信部

4 6 2, 4 7 2, 4 8 2 … 送信部

4 6 3, 4 7 3, 4 8 3 … 暗号化部

4 6 4, 4 7 4, 4 8 4 … 復号部

4 6 5, 4 7 5, 4 8 5 … 記憶部

4 6 6, 4 7 6, 4 8 6 … 制御部

4 6 7, 4 7 7 … 署名検証部

4 8 7 … 署名作成部

4 8 8 … 課金処理部

a 1 … 発注情報

k 1 … 発注者 3 1 の個人キー情報 k 1

I D 1 … 発注者 3 1 の個人 I D 情報

I D _ N … ネットワーク I D

A u 1, A u 2 … 認証装置の署名情報

Z … 受注者を特定する情報

I n f 1 … 認証要求

I n f 4 … 認証応答

This Page Blank (uspto)

5 0 1 … トランザクション認証システム
5 1 1 … 発注者端末装置
5 1 5 … 受注者端末装置
5 4 0 … ネットワーク銀行
5 5 0 … 認証装置
5 6 1 … 外部ネットワーク I / F
5 6 2 … 内部ネットワーク I / F
5 7 1, 5 8 1 … 受信部
5 7 2, 5 8 2 … 送信部
5 6 3, 5 7 3, 5 8 3 … 暗号化部
5 6 4, 5 7 4, 5 8 4 … 復号部
5 6 5, 5 7 5, 5 8 5 … 記憶部
5 6 6, 5 7 6, 5 8 6 … 制御部
5 6 7, 5 7 7 … 署名検証部
5 8 7 … 署名作成
5 8 8 … 課金処理部
a 1 … 発注情報
k 1 … 発注者 3 1 の個人キー情報 k 1
I D 1 … 発注者 3 1 の個人 I D 情報
I D_{M1}, I D_{M2}, I D_{M3}, I D_{M4}, I D_{M56} … 装置 I D 情報
A u 1, A u 2 … 認証装置の署名情報
Z … 受注者を特定する情報
I n f 1 … 認証要求
I n f 4 … 認証応答

This Page Blank (uspto)

- 6 0 1 …情報記録装置
- 6 1 0 …読み出し回路
- 6 1 1 …暗号化回路
- 6 1 2 …情報分割回路
- 6 1 3, 6 1 4 …書き込み回路
- 6 1 5, 6 1 6, 6 1 7 …記録媒体
- 6 2 0, 6 2 1 …読み出し回路
- 6 2 2 …情報合成回路
- 6 2 3 …復号回路
- 6 2 4 …書き込み回路
- 6 3 1 …情報復元装置
- 6 4 1 …情報記録装置
- 6 5 0 …読み出し回路
- 6 5 1 …情報分割回路
- 6 5 2, 6 5 3 …暗号化回路
- 6 5 4, 6 5 5 …書き込み回路
- 6 6 1 …情報復号装置
- 6 7 0, 6 7 1 …読み出し回路
- 6 7 2, 6 7 3 …復号回路
- 6 7 4 …情報合成回路
- 6 7 5 …書き込み回路

- 8 0 1 …認証システム
- 8 1 1 …端末装置
- 8 1 3 …認証装置
- 8 2 1 …ネットワーク銀行

This Page Blank (USP10)

- 8 3 1 … ユーザ
- 8 6 1, 8 8 1 … 受信部
- 8 6 2, 8 8 2 点送信部
- 8 6 3, 8 8 3 … 暗号化部
- 8 6 4, 8 8 4 … 復号部
- 8 6 5, 8 8 5 … 記憶部
- 8 6 6, 8 8 6 … 記憶部
- 8 6 7, 8 8 7 … 表示部
- 8 6 8, 8 8 8 … 制御部
- 8 6 9, 8 8 9 … スマートカードアクセス部

- 9 0 1 … トランザクション認証システム
- 9 1 1 … 発注者端末装置
- 9 1 1 a … 認証要求入力部
- 9 1 1 b … 認証要求送信部
- 9 1 1 c … 認証応答受信部
- 9 1 1 d … 認証要求暗号化部
- 9 1 1 e … 認証応答復号部
- 1 2 … 生体認証装置
- 9 1 3 … 認証装置
- 9 1 3 a … 認証要求受信部
- 9 1 3 b … 発注者認証部
- 9 1 3 c … 要求生成部
- 9 1 3 d … 要求送信部
- 9 1 3 e … 応答受信部
- 9 1 3 f … 受注者認証部

This Page Blank (uspto)

9 1 3 g … 認証応答生成部
9 1 3 h … 認証応答暗号化部
9 1 3 i … 認証応答送信部
9 1 3 j … 要求暗号化部
9 1 3 k … 応答復号部
9 1 3 l … 認証要求復号部
9 1 3 m … 決済処理部
9 1 3 n … 決済処理部
9 1 4 … 認証履歴格納装置
9 1 5 … 受注者端末装置
1 1 5 a … 認証要求受信部
1 1 5 b … 要求復号部
1 1 5 c … 応答入力部
1 9 1 5 d … 応答生成部
9 1 5 e … 応答暗号化部
9 1 5 f … 応答送信部

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00772

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F17/60, G09C1/00, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F17/60, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JOIS (JICST)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, 6006439, A (Citicorp Developmet Center, Inc.), 28 December, 1999 (28.12.99), Full text; Figs. 1 to 14 & GB, 9819879, A0 & EP, 917119, A2 & CN, 1233804, A & BR, 9806416, A & WO, 99024891, A2 & JP, 11-250165, A	1-72, 89-157
P,Y	JP, 2000-322484, A (Web Intelligence Network K.K.), 24 November, 2000 (24.11.00), Full text; Figs. 1 to 17 (Family: none)	1-72, 89-157
Y	JP, 10-282883, A (Oki Electric Industry Co., Ltd.), 23 October, 1998 (23.10.98), Full text; Figs. 1 to 6 & US, 6148404, A	24-72
Y	JP, 11-328117, A (Hitachi, Ltd.), 30 November, 1999 (30.11.99), Full text; Figs. 1 to 9 (Family: none)	24-72
Y	JP, 2000-029792, A (Hitachi, Ltd.), 28 January, 2000 (28.01.00),	73-88, 158-174

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search
17 April, 2001 (17.04.01)Date of mailing of the international search report
01 May, 2001 (01.05.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Full text; Figs. 1 to 6 (Family: none)	
Y	JP, 10-336169, A (Nippon Yunishisu K.K.), 18 December, 1998 (18.12.98), Full text; Figs. 1 to 19 & US, 6148404, A	73-88, 158-174
P,Y	JP, 2000-353194, A (Hitachi, Ltd.), 19 December, 2000 (19.12.00), Full text; Figs. 1 to 15 (Family: none)	73-88, 158-174
Y	EP, 0884669, A2 (Mitsubishi Corporation), 16 December, 1998 (16.12.98), Full text; Figs. 1 to 10 & JP, 11-007241, A	89-105, 120-157
P,Y	JP, 2000-174796, A (Hitachi, Ltd.), 23 June, 2000 (23.06.00), Full text; Figs. 1 to 7 (Family: none)	89-105, 120-157
Y	JP, 2000-029841, A (Aibikkusu K.K.), 28 January, 2000 (28.01.00), Full text; Figs. 1 to 2	106-119

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00772

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature of the inventions of claims 1-6 is that, in a transaction authentication system, a transaction authentication agent, being a third party of an electronic transaction between the concerned parties, an orderer and an order acceptor, intervenes between the concerned parties of the electronic transaction and sends information from which personal key information is excluded from an authentication apparatus to an order-accepter device, and therefore unauthorized use of personal key information is prevented.

The technical feature of the inventions of claims 7-23 is that, in a transaction authentication system, a transaction authentication agent, being a third party of an electronic transaction, intervenes between the concerned parties of the electronic transaction, an orderer and an order-accepter, and therefore the reliability of electronic transaction is enhanced.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00772

Continuation of Box No.II of continuation of first sheet (1)

The technical feature of the inventions of claims 24-44 is that, in a transaction authentication system, when transaction parties are under contract with respective different authentication institutions, the authentication apparatuses do authentication in cooperation with one another.

The technical feature of the inventions of claims 45-72 is that, in a transaction authentication system, when transaction parties are under contract with respective different authentication institutions, the authentication apparatus do authentication in cooperation with one another, information from which personal key information is excluded is sent from the authentication apparatus of the orderer to the order-accepter apparatus, and therefore unauthorized use of the personal key information is prevented.

The technical feature of the inventions of claims 73-88 is that, in an authentication system, the user authentication information is divided into a first set of authentication information and a second set of authentication information, the second set of authentication information is stored in a portable memory device that the user holds, the authentication information is restored by using the first set of authentication information received from the authentication apparatus and the second set of authentication information read from the portable memory device, and therefore any false user cannot obtain the authentication information thereby to prevent unauthorized use such as imposture.

The technical feature of the inventions of claims 89-105 is that, in a transaction authentication system, personal identification information is correlated with information about the destination to which the processing result is to be sent, the personal identification information and the destination information is stored, the processing result is sent to the destination specified by the destination information, and thereby when any false person who has fraudulently obtained the personal information about the orderer sends an authentication request to the authentication apparatus, the orderer can know that an unauthorized transaction using the orderer's personal information is carried out.

The technical feature of the inventions of claims 106-119 is that, in a transaction authentication system, an authentication apparatus manages the information about the history of a series of procedures conducted between an orderer and an order acceptor, and therefore a plurality of payments for one order can be effectively prevented.

The technical feature of the inventions of claims 120-137 is that, in a communication system, a communication control device sends device identification information corresponding to a first communication device to a second communication device, receives information for identifying the sender device from the second communication device, judges whether or not the received device identification information agrees with the stored device identification information, and judges, based on the agreement judgment, whether or not the first communication device is an authorized one, thereby to detect an unauthorized request.

The technical feature of the inventions of claims 138-157 is that, in a transaction authentication system, personal identification information is correlated with information about the destination to which the processing result is to be sent, the personal identification information and the destination information is stored, the authentication result is sent to the destination specified by the destination information, and thereby when any false person who has fraudulently obtained the order's personal information sends an authentication request to the authentication apparatus, the orderer can know that an unauthorized transaction using the orderer's personal information is carried out.

The technical feature of the inventions of claims 158-174 is that predetermined information is divided into modules, the modules are recorded on different recording media or on different areas of one recording medium, and thereby the secrecy of the predetermined information is maintained and the secret predetermined information is restored from the modules.

These groups of inventions are not united into one invention nor so linked as to form a single general inventive concept.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60, G09C1/00, H04L9/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60, G09C1/00, H04L9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JOIS (JICST)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	US, 6006439, A (Citicorp Developmet Center, Inc.) 28. 12月. 1999 (28. 12. 99) 全文, 第1-14図 & GB, 9819879, A0 & EP, 9171119, A2 & CN, 1233804, A & BR, 9806416, A & WO, 99024891, A2 & EP, 950972, A & AU, 1584499, A & JP, 11-250165, A	1-72, 89-157
P, Y	JP, 2000-322484, A (ウェブインテリジェンスネット ワーク株式会社) 24. 11月. 2000 (24. 11. 00) 全文, 第1-17図 (ファミリーなし)	1-72, 89-157

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

17. 04. 01

国際調査報告の発送日

01.05.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丹治 彰



5L

8320

電話番号 03-3581-1101 内線 3560

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 10-282883, A (沖電気工業株式会社) 23. 10月. 1998 (23. 10. 98) 全文, 第1-7図 (ファミリーなし)	24-72
Y	JP, 11-328117, A (株式会社日立製作所). 30. 11月. 1999 (30. 11. 99) 全文, 第1-9図 (ファミリーなし)	24-72
Y	JP, 2000-029792, A (株式会社日立製作所) 28. 1月. 2000 (28. 01. 00) 全文, 第1-6図 (ファミリーなし)	73-88, 158- 174
Y	JP, 10-336169, A (日本ユニシス株式会社) 18. 12月. 1998 (18. 12. 98) 全文, 第1-19図 & US, 6148404, A	73-88, 158- 174
P, Y	JP, 2000-353194, A (株式会社日立製作所) 19. 12月. 2000 (19. 12. 00) 全文, 第1-15図 (ファミリーなし)	73-88, 158- 174
Y	EP, 0884669, A2 (Mitsubishi Corporation) 16. 12月. 1998 (16. 12. 98) 全文, 第1-10図 & JP, 11-007241, A	89- 105, 120- 157
P, Y	JP, 2000-174796, A (株式会社日立製作所) 23. 6月. 2000 (23. 06. 00) 全文, 第1-7図 (ファミリーなし)	89- 105, 120- 157
Y	JP, 2000-029841, A (アイビックス株式会社) 28. 1月. 2000 (28. 01. 00) 全文, 第1-2図 (ファミリーなし)	106- 119

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-6は、トランザクション認証システムにおいて、電子商取引の当事者である発注者と受注者との間にその商取引の第三者であるトランザクション認証局が介在し、認証装置から受注者装置に個人キー情報を除去して送信するため、個人キー情報の不正利用を抑制できることを技術的特徴とするものである。

請求の範囲7-23は、トランザクション認証システムにおいて、電子商取引の当事者である発注者と受注者との間にその商取引の第三者であるトランザクション認証局が介在することにより、電子商取引の信頼性を高めることを技術的特徴とするものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

(第II欄の続き)

請求の範囲24-44は、トランザクション認証システムにおいて、複数の取引者がそれぞれ異なる認証機関と契約を行っている場合に、複数の認証装置間で連携して認証処理を行うことを技術的特徴とするものである。

請求の範囲45-72は、トランザクション認証システムにおいて、複数の取引者がそれぞれ異なる認証機関と契約を行っている場合に、複数の認証装置間で連携して認証処理を行うものであって、発注者の認証装置から受注者装置に個人キー情報を除去して送信するため、個人キー情報の不正利用を抑制できることを技術的特徴とするものである。

請求の範囲73-88は、認証システムにおいて、ユーザの認証情報を第1の認証情報及び第2の認証情報に分割し、第2の認証情報をユーザの保持する携帯型メモリ装置に記憶し、認証装置から受信した第1の認証情報と携帯型メモリ装置から読み出した第2の認証情報とを用いて認証情報を復元することにより、不正なユーザは認証情報を得ることが出来ず、なりすましなどの不正利用を防止できることを技術的特徴とするものである。

請求の範囲89-105は、トランザクション認証システムにおいて、個人識別情報と処理結果を送信する送信先の情報とを対応づけて記憶し、処理の結果を送信先に情報によって特定された送信先に送信することにより、発注者の個人情報をも不正に取得したものが認証装置に認証要求を行った場合に、発注者は自らの個人情報を用いた不正な取引が行われることを知ることができることを技術的特徴とするものである。

請求の範囲106-119は、トランザクション認証システムにおいて、認証装置が発注者および受注者との間で行われた一連の手続きの履歴情報を管理するため、一つの受注に対して複数回の引き落としが行われることを効果的に回避できることを技術的特徴とするものである。

請求の範囲120-137は、通信システムにおいて、第1の通信装置に対応する装置識別情報を第2の通信装置に送信し、第2の通信装置から送信元の装置を識別するための情報を受信して、受信した装置識別情報と記憶された装置識別情報とが一致するか否かに基づいて、第1の通信装置が正当なものであるか否かを判断することにより、不正な要求が行われたことを検出できることを技術的特徴とするものである。

請求の範囲138-157は、トランザクション認証システムにおいて個人識別情報と処理結果を送信する送信先の情報とを対応づけて記憶し、認証処理の結果を送信先に情報によって特定された送信先に送信することにより、発注者の個人情報をも不正に取得したものが認証装置に認証要求を行った場合に、発注者は自らの個人情報を用いた不正な取引が行われることを知ることができることを技術的特徴とするものである。

請求の範囲158-174は、所定の情報を複数のモジュールに分割し、相互に異なる記録媒体または同一の記録媒体の異なる領域に記録することにより、所定の情報の秘匿性を保持するとともに、複数のモジュールから秘匿された所定の情報を復元することを技術的特徴とするものである。

これらは、一の発明であるとも、単一の一般的発明概念を形成するように連関している一群の発明であるとも認められない。